# 虚拟专用网

【实验目的】

（1）通过对木马的练习，使读者理解和掌握木马传播和运行的机制；

（2）通过手动删除木马，掌握检查木马和删除木马的技巧，学会防御木马的相关知识，加深对木马的安全防范意识。

【实验仪器】

 两台运行Windows2000 系统的计算机，通过局域网连接。使用“冰河”木马作为练习工具。

【实验原理】

木马的攻击与检测

  木马是隐藏在正常程序中的具有特殊功能恶意代码，是具备破坏，删除和修改文件，发送密码，记录键盘，实施Dos攻击甚至完全可能告知计算机等特殊功能的后门程序。它隐藏在目标计算机里，可以随计算机自动启动并在某一端口监听来自控制端的控制信息。

木马工作原理

  木马的传统连接技术 一般木马都采用C/S(client/server,即服务器/客户端)运行模式，因此它分为两部分，即客户端和服务前端木马程序。其原理是，当服务器端程序在目标计算机上被执行后，一般会打开一个默认的端口进行监听，当客户端向服务器端主动提出连接请求，服务器端的木马程序就会自动运行，来应答客户端的请求，从而建立连接。第一代和第二代木马就采用这种方式。

  木马的反弹端口技术 随着防火墙技术的发展，它可有效拦截从外部主动发起的连接的木马程序。但防火墙对内部发起的连接请求则认为是正常连接，第三代第四代木马就是利用这个缺点，其服务器端程序主动发起对外连接请求，再通过某些方式连接到木马的客户端，就是说“反弹式”木马是服务器端主动发起连接请求，而客户端是被动的连接。

  线程插入技术，我们知道，一个应用程序在运行之后，都会在系统之中产生一个进程，同时，每个进程分别对应了一个不同的进程标识符。系统会分配一个虚拟的内存空间地址段给这个进程，一切相关的程序操作，都会在这个虚拟的空间中进行。一般情况下，线程之间是相互独立的，当一个线程发生错误的时候，并不一定会导致整个进程的崩溃。“线程插入”技术就是利用线程之间运行的相对独立性，使木马完全地融进了系统那个内核。系统运行时会有很多的进程，而每个进程又有许多的线程，这就导致了查杀利用“线程插入”技术木马程序的难度。

【实验任务和步骤】

1实验步骤一：1.1启动实验平台，拖出Windows PC机，并启动进入虚拟机环境，如图4-1所示：

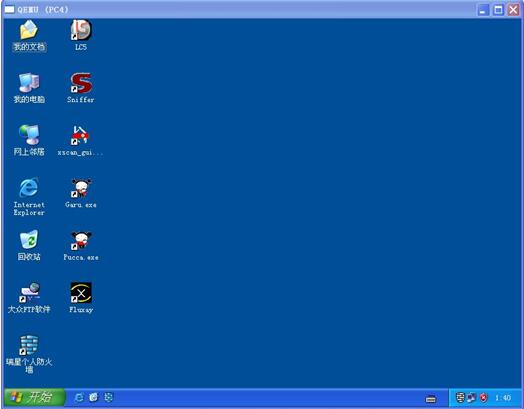


                   图4-1 虚拟机界面

2步骤二：冰河木马的攻击

   “冰河”一般是由两个文件组成：Garu.exe和Pucca.exe，其中IMG_257是木马的服务器端，即用来植入目标主机的程序,IMG_258是木马的客户端，即木马的控制端.

我们在一台目标主机上植入木马，也即在此主机上运行Pucca.exe，作为服务器端；在另一台主机运行G\_Client，作为控制端,打开控制端Garu.exe，弹出“冰河”的主界面，如图4-2所示：

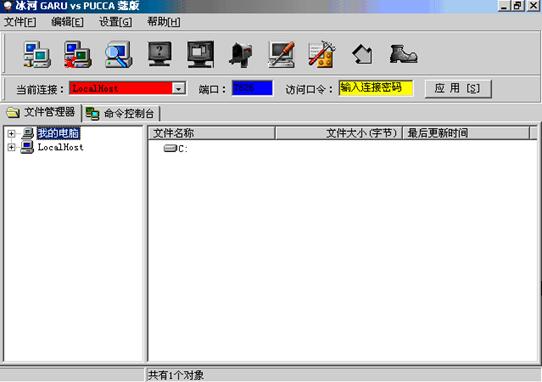


                     图4-2 冰河主界面

单击快捷工具栏中的“添加主机”按钮IMG_260，弹出如图4-11所示对话框：



      图4-3 添加计算机

显示名称：填入显示在主界面的名称

主机地址：填入服务器端主机的IP地址

访问口令：填入每次访问主机的密码，“空”即可

监听端口：冰河默认的监听端口是7626，控制端可以修改它以绕过防火墙，单击确定按钮，即可以看到主机界面上添加了192.168.2.20的

主机。如图4-4所示：

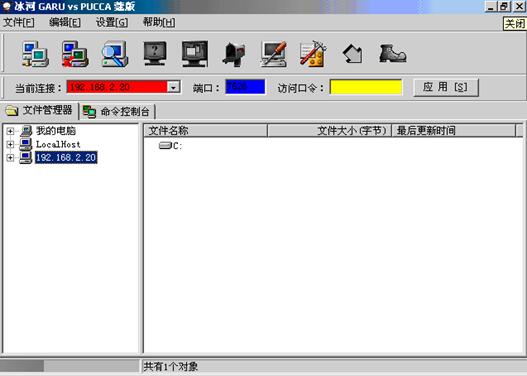


              图4-4  添加192.168.2.20主机

单击192.168.2.20主机，如果连接成功，则会显示服务器端主机上的盘符。这时我们就可以像操作自己的电脑一样操作远程目标电脑，比如打开C:\WINNT\system32\config目录可以找到对方主机上保存用户口令的SAM文件。

   命令控制台分为“口令类命令”，“控制类命令”，“网络类命令”，“文件类命令”，“注册表读写”，“设置类命令”。下面我们简单介绍几个命令的使用方法：

(1)口令类命令： 展开控制类命令，如图4-5所示：



                    图4-5 口令类命令

“系统信息及口令”：可以查看远程主机的系统信息，开机口令，缓存口令等。可看到非常详细的远程主机信息，这就无异于远程主机彻底暴露在攻击者面前，系统信息如图4-6：



                    图4-6 系统信息示图

“历史口令”：可以查看远程主机以往使用的口令

“击键记录”：启动键盘记录后，可以记录远程主机用户击键记录，一次可以分析出远程主机的各种账号和口令或各种秘密信息

（2）控制类命令，展开控制类命令

“捕获屏幕”：这个功能可以使控制端使用者查看远程主机的屏幕，好像远程主机就在自己面前一样，这样更有利于窃取各种信息，单击“查看屏幕”按钮，然后就染成了远程主机的屏幕，可以看到，远程主机屏幕上的内容就显示在本机上了，显示内容不是动态的，而是每隔一段时间传来一幅，如图4-7所示：



                图4-7 捕获远程主机屏幕

“发送信息”：这个功能可以使你向远程计算机发生Windows标准的各种信息，在“信息正文”中可以填入要发给对方的信息，在图表类型中，可以选择“普通”，“警告”，“询问”，“错误”等类型。按钮类型可以选择“确定”“是”“否”等类型。如图4-8所示：



                    图4-8 发送信息示图

“进程管理”：这个功能可以使控制着查看远程主机上所有的进程，如图4-9：



                 图4-9  进程查看示图

“窗口管理”：这个功能可以使远程主机上的窗口进行刷新，最大化，最小化，激活，隐藏等操作:

“系统管理”：这个功能可以使远程主机进行关机，重启，重新加载“冰河”自动卸载“冰河”的操作

“鼠标控制”：这个功能可以使远程主机上的鼠标锁定在某个范围内

“其他控制”：这个功能可以使远程主机进行自动拨号禁止，桌面隐藏，注册表锁定等操作

（3）网络类命令

“创建共享”：在远程主机上创建自己的共享

“删除共享”：在远程主机上删除某个特定的共享

“网络信息”：查看远程主机上的共享信息

(4)  文件类命令 展开“文件类命令”，“文件浏览”，“文件查找”，“文件压缩”，“文件删除”，“文件打开”等菜单可以查看，查找，压缩，删除，打开远程主机上某个文件。“目录增删”，“目录复制”，可以增加，删除，复制远程主机上的某个目录。

(5) 注册表读写 展开“注册表读写”，注册表读写提供了“键值读取”，“键值写入”,“键值重命名”，“主键浏览”，“主键增删”“主键复制”的功能

(6)  设置类命令 展开“设置类命令”，设置类命令提供了“更换墙纸”，“更改计算机名”“服务器端配置”的功能，如图4-10 所示：



                 图4-10设置类命令示图

3 删除冰河木马

删除冰河木马主要有以下几种方法：

客户端的自动卸载功能 在“控制类命令”中的“系统控制”里面就有自动卸载功能，执行这个功能，远程主机上的木马就自动卸载了。

手动卸载  在实际情况中木马客户端不可能为木马服务器端自动卸载木马，我们在发现计算机有异常情况时，（如经常自动重启，密码信息泄露时）就应该怀疑是否已经中了木马，这时我们应该查看注册表，在“开始”的“运行”里面输入regedit，打开Windows注册表编辑器。依次打开子键目录：HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,如图4-11所示：

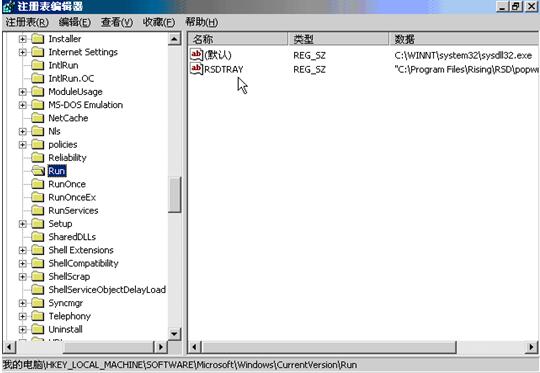


                 图4-11  注册表Run子键目录示图

在目录中发现了一个默认的键值C:\WINNT\System32\Sysdll32.exe，这就是“冰河”密码在注册表中加入的键值，将它删除。然后依次打开子键目录：    HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runservices，如图4-20所示：

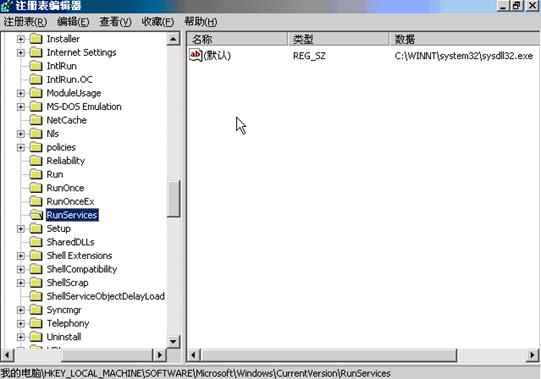


                图4-12 注册表Runservices子键目录示图

在目录中也发现了一个默认的键值C:\WINNT\System32\Sysdll32.exe，这也是“冰河”木马在注册表中加入的键值，将它删除。上面两个注册表的子键目录Run和Runservices中存放的键值是系统启动时自动起订的程序，一般病毒程序，木马程序，后门程序等都放在这些子键目录下，所以要经常检查这些子键目录下的程序，如果有不明程序，要着重进行分析。

然后我们再进入C:\WINNT\System32目录，找到“冰河”木马的两个可执行文件Kernel32.exe和Sysdll32.exe文件，将它们删除，如图4-13和4-14

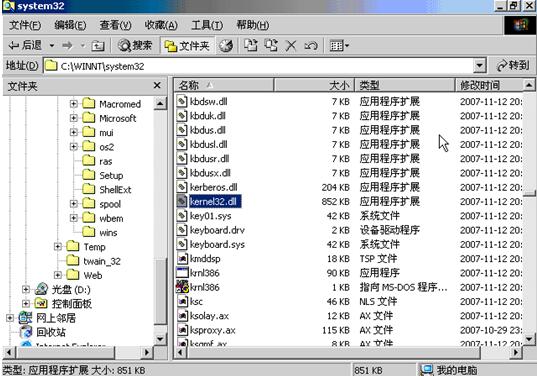


                图4-13 Kernel32.exe文件

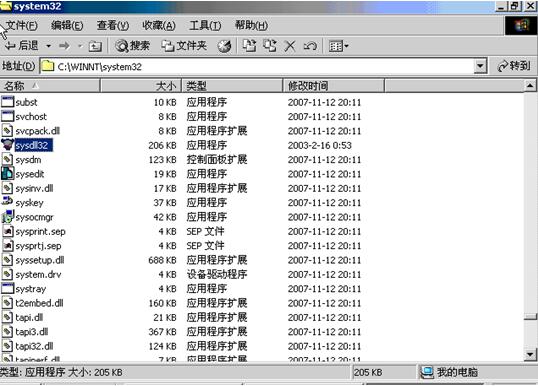


                 图4-14 Sysdll32.exe文件

修改文件关联也是木马常用的手段，“冰河”木马将txt文件的缺省打开方式由notepad.exe改为木马的启动程序，除此之外，html,exe,zip,com等也都是木马的目标，所以，在最后需要回复注册表中的txt文件关联功能，只要将注册表的HKEY\_CLASSES\_ROOT\txtfileShell\open\command下的默认值，由中木马后的C:\Windows\System\Sysexplr.exe%1改为正常情况下的C:\Windows\notepad.exe%1即可。

重新启动计算机，冰河木马就彻底删除了。

杀毒软件查杀 大部分杀毒软件都有查杀木马的功能，可以通过这个功能对主机进行全面扫描来去除木马。