实验五　冰河木马

1.实验目的

通过对木马的练习，理解与掌握木马传播与运行的机制；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。

2.实验原理

木马的全称为特洛伊木马，源古希腊神话。木马是隐藏在正常程序中的具有特殊功能的恶意代码，它具备破坏、发送密码、记录键盘、实施 DOS 攻击甚至完全控制计算机等特殊功能的后门程序。它隐藏在目标计算机中，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。

1　木马的入侵途径

http://zhidao.baidu.com/question/5028639.html

2　木马的工作原理

https://blog.csdn.net/qq_40927867/article/details/104596357

3.实验环境

两台运行 Windows 2000/XP 的计算机，通过网络连接。使用“冰河”木马作为练习工具。

4.实验内容和任务

冰河可以从 ftp 下载。

冰河使用图文教程

https://wenku.baidu.com/view/3ac9e7f44693daef5ef73d6f.html

注意：进行如下任务前先将杀毒软件的监控模块关闭，否则杀毒软件会将这两个木马程序清除，而导致实验无法进行。

任务一　使用冰河对远程计算机进行控制

在一台目标主机上植入木马，在此主机上运行 G_server，作为服务器端；在另一台主机上运行 G_Client，作为控制端。

具体步骤如下：

在一台目标主机上植入木马，在此主机上运行 G_Server，作为服务器端，在另一台主机上运行 G_Client 作为控制端。植入木马后的目标主机可看到 7626 端口开放，如图 A.1 所示，这是冰河木马的默认使用端口。

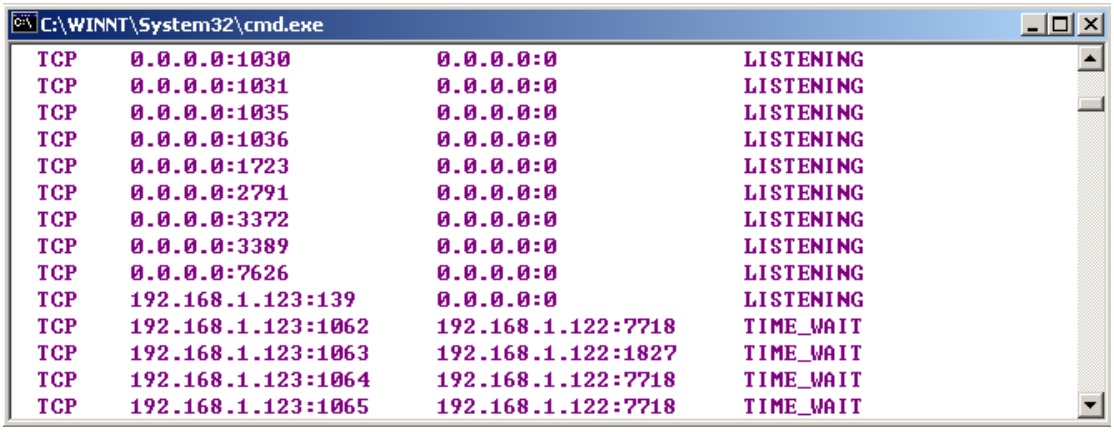

图 A.1 冰河的默认端口

打开控制端程序，单击“添加主机”按钮，弹出如下图所示对话框

图 A.2 冰河控制端添加主机

“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，即可以看到主界面上添加了 wan 的主机，如下图所示。(截图)

图 A.3 添加主机后的界面

单击主机名，如果连接成功，则会显示服务器端主机上的盘符。如图 A.4 所示(截图)

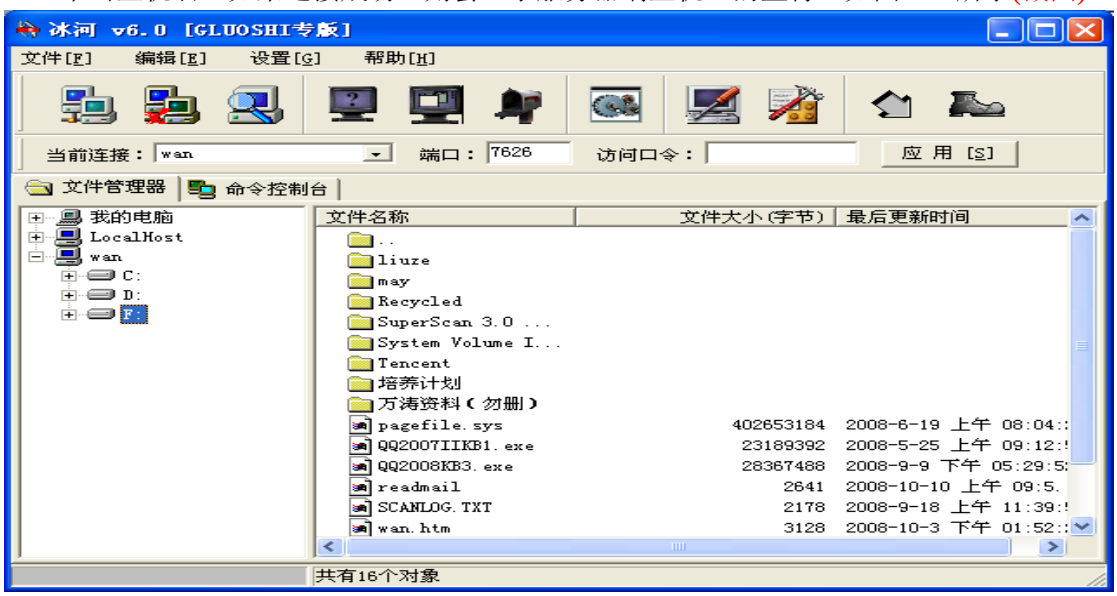

图 A.4 连接成功界面

这时就可以像操作自己的电脑一样操作远程目标电脑。

“冰河”的大部分功能都在“命令控制台”实现，单击“命令控制台”标签，弹出如图 A.5 所示命令控制台界面(完成其中不同类型的命令若干(不少于 6 个)，并截图)

图 A.5 控制台界面

可以看到命令控制台分为“口令类命令”、“控制类命令”、“文件类命令”、“注册表读写”、“设置类命令”。下面介绍几个命令的使用方法。

（1）口令类命令 展开“口令类命令”如图 A.6 所示

图 A.6 口令类命令

①“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，如图 A.7 所示。单击“系统信息”按钮，可以看到远程主机的 Windows 版本，当前用户，内存容量等，还可以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。

图 A.7 系统信息及口令

②“历史口令”：可以查看远程主机以往使用的口令。

③“击键记录”：启动键盘记录后，可以记录远程用户击键记录，以此可以分析出远程主机的各种帐号和口令或各种秘密信息。

（2）控制类命令 展开“控制类命令”如图 A.8 所示

图 A.8 控制类命令

① “捕获屏幕”：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”，然后就弹出了远程主机的屏幕如图 A.9 所示。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，而是每隔一段实践传来一幅。

②“发送信息：可以使控制端使用者向远程计算机发送 Windows 标准的各种信息。

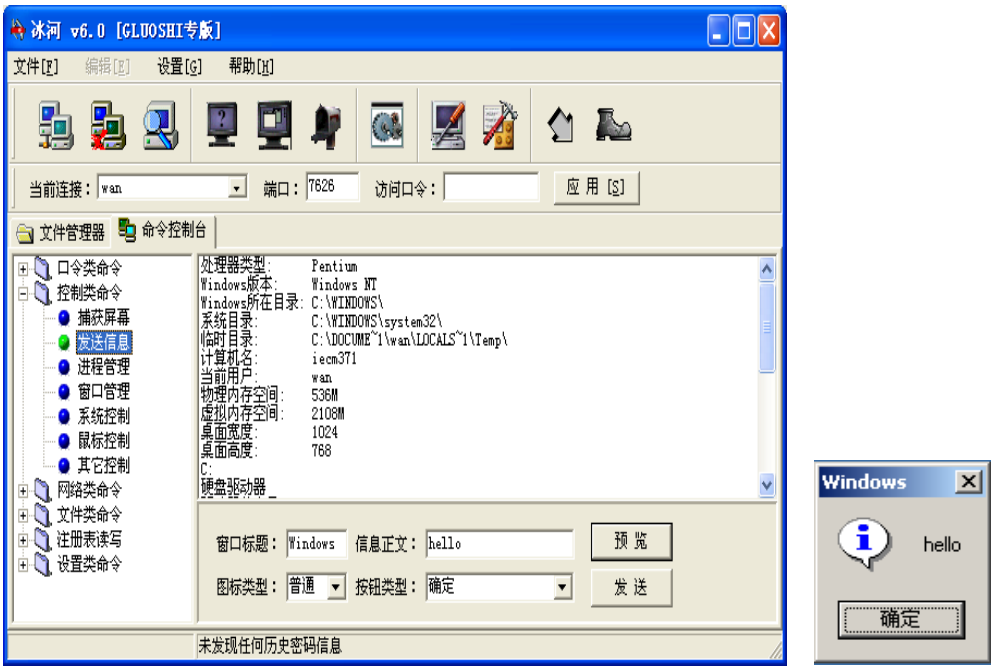

图 A.9 查看屏幕结果

③“进程管理”：可以使控制端使用者查看远程主机上的所有进程，如图 A.10 所示。可以查看远程主机上存在的进程也可以终止某个进程。

图 A.10 进程管理

④“窗口管理”：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。

⑤“系统管理”：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”操作。

⑥“鼠标控制”：可以使远程主机上的鼠标锁定在某个范围内。

⑦“其他控制”：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 展开“网络类命令”，如图 A.11 所示。

“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。

图 A.11 网络类命令

（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、复制远程主机上某个目录。

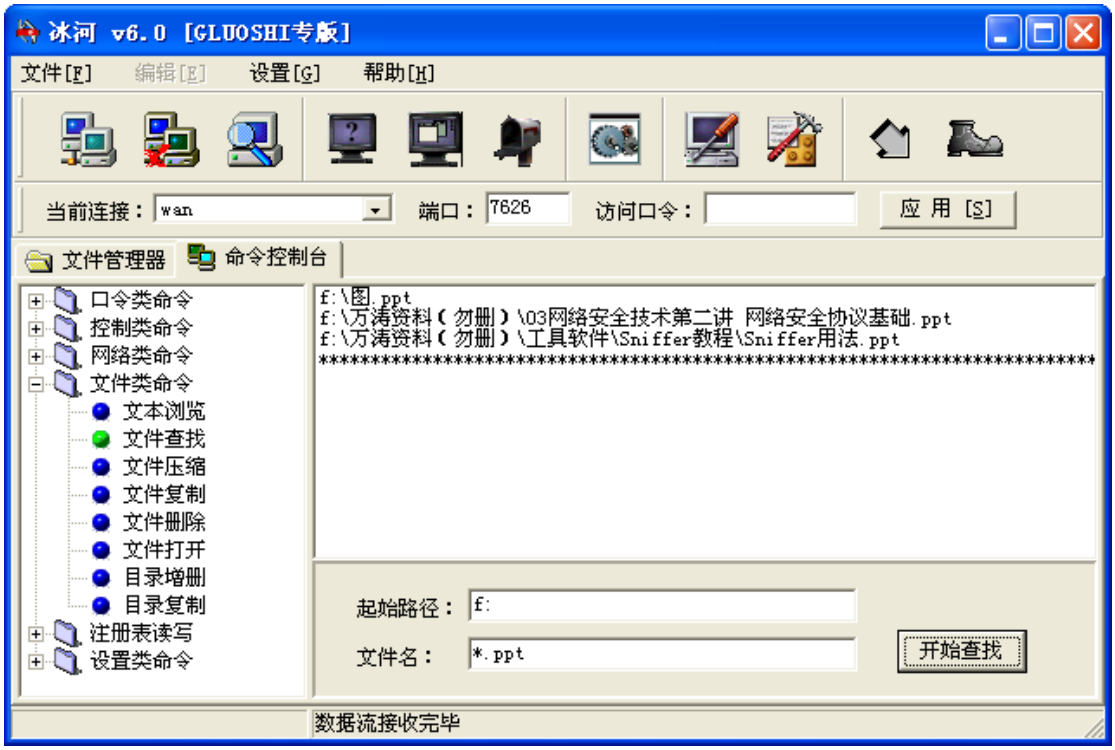

图 A.12 文件类命令

（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。

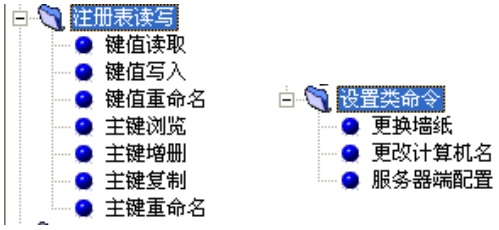

图 A.13 注册表读写

（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”、“更换计算机名”、“服务器端配置”的功能。

任务二 手动删除冰河木马

步骤 1：查看注册表中木马踪迹

在命令行窗口运行 Regedit 命令打开注册表编辑器，在:

KEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

查看键值中没有自己不熟悉自动启动文件，扩展名为 EXE。

一般“冰河”的默认文件名为 KERNEL32.EXE（注意此文件的名字可能会被种马的人改变）。

如果有，那我们现在开始进行修改，先删除该键值中这一项，再删除 RUNDRIVES 这个键值。

一般“冰河”用户端程序的自我保护设为：关联 TXT 文件或 EXE 文件，关联的文件为：SYSEXPLR.EXE。

步骤 2：去掉文本文件或 EXE 文件关联

A.在“查看”菜单中选择“文件夹选项”弹出文件夹选项对话框，选择“文件类型” 在“已注册文件类型”框中找到“TXT FILE”这一项，看一下“打开方式”有无变化（一般为：NOTEPAD），如果关联对象不是 NOTEPAD，选择“编辑”按钮，在“操作”框中删除“OPEN”这一项，这样关联 TXT 文件的用户程序就失效了。

B、如果是关联的 EXE 文件，首先打开注册表编辑器，在:HKEY_CLASSES_ROOT\.exe 中把 “默认”的键值随便改成什么(注意看清楚，等会儿要改回来)。

以上这两步做完后，退出 WINDOWS，在 DOS 状态下删除该“冰河”用户端程序，重新启动即可。

5.实验报告要求

要求对实验过程中的每一步都要有对应的实验结果截图，并要有详细的说明。拒绝抄袭。