浅谈用VB6.0编写木马程序 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/136/2021_2022__E6_B5_85_E8_B0_88_E7_94_A8V_c97_136803.htm 现在网络上流行的木马软件基本都是客户机/服务器模式也就是所谓的C/S结构，目前也有一些开始向B/S结构转变，在这里暂且不对B/S结构进行详谈，本文主要介绍C/S结构其原理就是在本机直接启动运行的程序拥有与使用者相同的权限。因此如果能够启动服务器端（即被攻击的计算机）的服务器程序，就可以使用相应的客户端工具客户程序直接控制它了。下面来谈谈如何用VB来实现它。 首先使用VB建立两个程序，一个为客户端程序Client，一个为服务器端程序systry。 在Client工程中建立一个窗体，加载WinSock控件，称为tcpClient，协议选择TCP，再加入两个文本框，用以输入服务器的IP地址或服务器名，然后建立一个按钮，按下之后就可以对连接进行初始化了，代码如下： Private Sub cmdConnect_Click() If Len(Text1.Text) = 0 And Len(Text2.Text) = 0 Then MsgBox ("请输入主机名或主机IP地址。") Exit Sub Else If Len(Text1.Text) > 0 Then tcpClient.RemoteHost = Text1.Text Else tcpClient.RemoteHost = Text2.Text End If End If tcpClient.Connect Timer1.Enabled = True End Sub 连接建立之后就可以使用DataArrival事件处理所收到的数据了。 在服务器端systry工程也建立一个窗体，加载WinSock控件，称为tcpServer，协议选择TCP，在Form_Load事件中加入如下代码： Private Sub Form_Load() tcpServer.LocalPort = 1999 tcpServer.Listen End Sub 准备应答客户端程序的请求连接，使用ConnectionRequest事件来应答户

端程序的请求，代码如下： Private Sub tcpServer_ConnectionRequest (ByVal requestID As Long) If tcpServer.State sckClosed Then tcpServer.Close ‘ 检查控件的 State 属性是否为关闭的。 End If ’ 如果不是，在接受新的连接之前先关闭此连接。 tcpServer.Accept requestID End Sub 