第11讲 5.3.29指针变量的值

1. 指针变量的值:

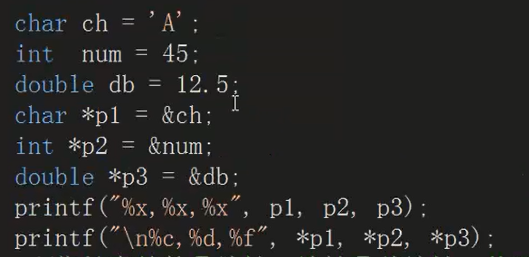
是指针本身存储的数值，这个值将被编译器当作一个地址，而不是   
一个一般的数值。在32位程序里，所有类型的指针的值都是一个32位整数，因为32位程序里内存地址长度都为32位。

指针所指向的内存区:

就是从指针的值所代表的那个内存地址开始，长度为sizeof(指针所指向的类型)的一片内存区。

指针存储的是地址，地址是首地址，从哪里开始，从哪里结束，由类型决定，

类型决定长度，决定如何解析。



2、自己编写外挂改变，通过另外一个程序改变这个进程。

在上面的代码中添加如下代码，使其打印数据:

while(1)

{

printf("我的级别是%c,我的年龄是%d,我的人民币是%fW",ch,num,db);

Sleep(5000);

}

要注入的dll程序

通过指针直接访问变量的地址，使其通过注入的方式，从而改变它的值，从而改变另一个程序的运行结果

