(86 条消息) C 语言野指针讲解_Rookie Linux 的博客-CSDN 博客_c 语言野指针

在实际工程开发中经常会听到“野指针”，那么问题来了，什么是野指针？野指针有什么危害？

在介绍野指针之前，先了解一点，**指针变量的本质是值，只不过这个值有点特殊，是一个内存地址值**

“野指针”指的是指针变量中的值是非法的内存地址，但“野指针”不是空指针（NULL），“野指针”指向的内存是不可用的，“野指针”往往会造成内存越界、段错误等问题

补充：合法的内存地址包括定义的变量的地址、malloc函数申请堆内存返回的地址（但未使用free释放）

介绍过“野指针”的概念后就该了解一下**“野指针”的由来**，这样在工程开发中我们就可以去**避免野指的产生**

1、局部指针变量没有初始化。因为局部变量不像全局变量那样，不赋值会自动初始化为0，所以局部指针变量不初始化话的话，指向的是一块程序员无法把控的内存，**我们在定义局部指针变量会初始化为NULL，局部变量初始化为0**

2、指针所指向的变量在指针使用之前就被销毁了。最常见的在函数调用结束后返回指向局部变量的指针，所以我们**绝对不要在函数中返回局部变量和局部数组的地址**，关于这种情况后续我再介绍堆栈的时候再举例说明

3、使用已经释放过的指针。比如malloc申请的堆空间通过free释放后又去调用该指针，**一定要在释放过后将指针变量的值赋值为NULL**

4、指针运算错误。比如有些情况下虽然初始化或者申请堆空间并未造成“野指针”，但是操作指针不当造成指针指向一块已经被别的进程使用的内存，**为避免这种情况，一定要确保字符数组要以'\0'结尾，自己编写的内存相关函数指定长度信息（防止内存越界）**

5、进行了错误的强制类型转换。比如我们在写嵌入式程序的时候，会将int类型的一个数据强制转换成一个指针类型用来表示寄存器的地址，这个时候有可能会因为这个数字取值不当，正好对应的内存已经被使用