# lab14\_kmemleak实验说明

学会使用kmemleak来检查内存泄漏。

## 基本实验步骤

1. 首先首先需要重新配置内核选项，打开CONFIG\_SLUB和CONFIG\_SLUB\_DEBUG\_ON这两个选项。

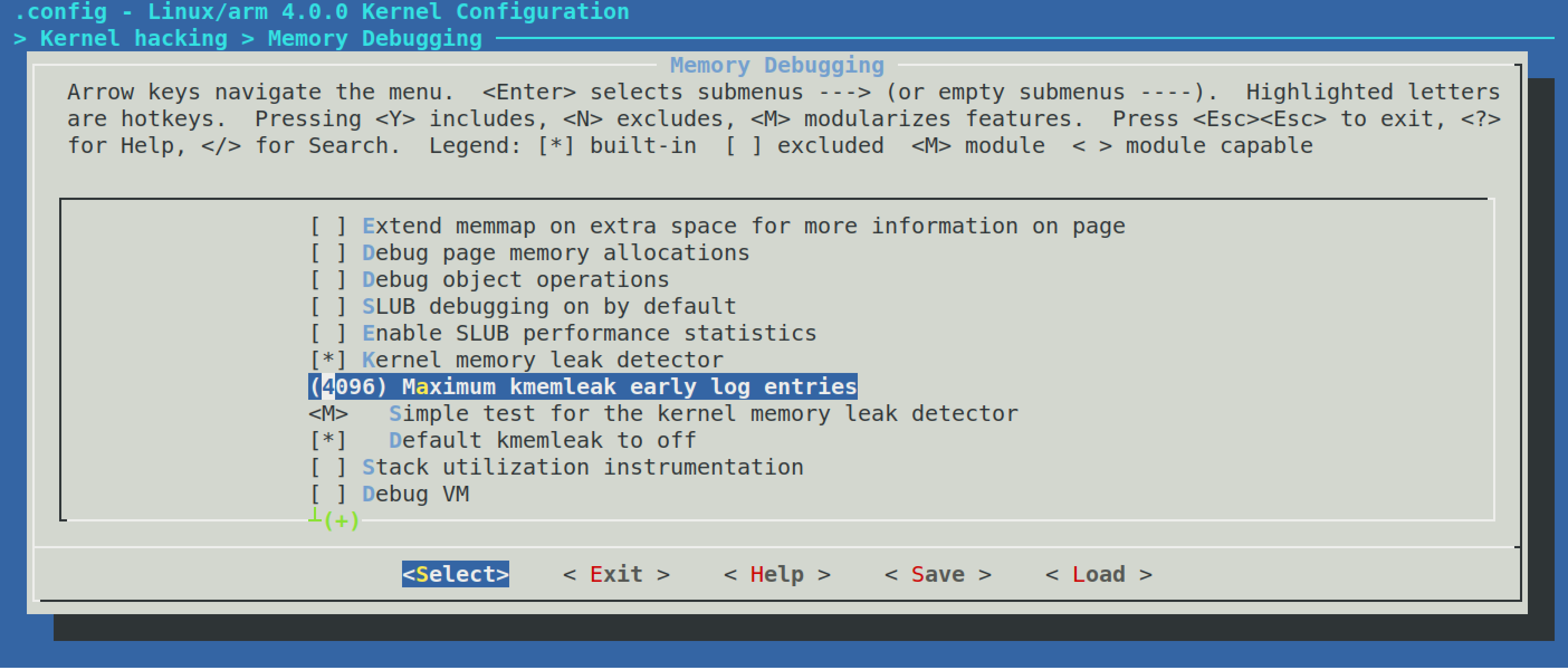
|  |
| --- |
| # export ARCH=arm  #export CROSS\_COMPILE=arm-linux-gnueabi-  # make vexpress\_defconfig  # make menuconfig |

然后在Kernel hacking-> Memory Debugging菜单中选中如下两项：

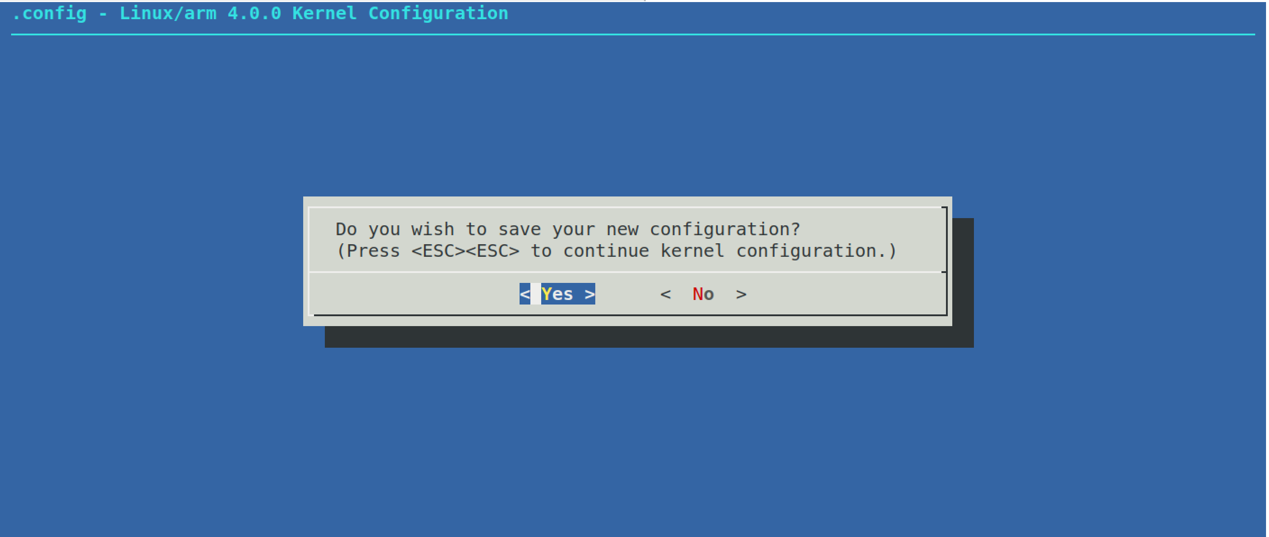
Kernel memory leak detector

Default kmemleak to off

Maximum kmemleak early log entries 设置4096, 这里不能设置太小,否则kmemleak不不成功.



退出时候选择“Yes”保存。



当然你不用menuconfig这种图形化的菜单，也可以手工修改config文件。

**[arch/arm/configs/vexpress\_defconfig]**

CONFIG\_HAVE\_DEBUG\_KMEMLEAK=y

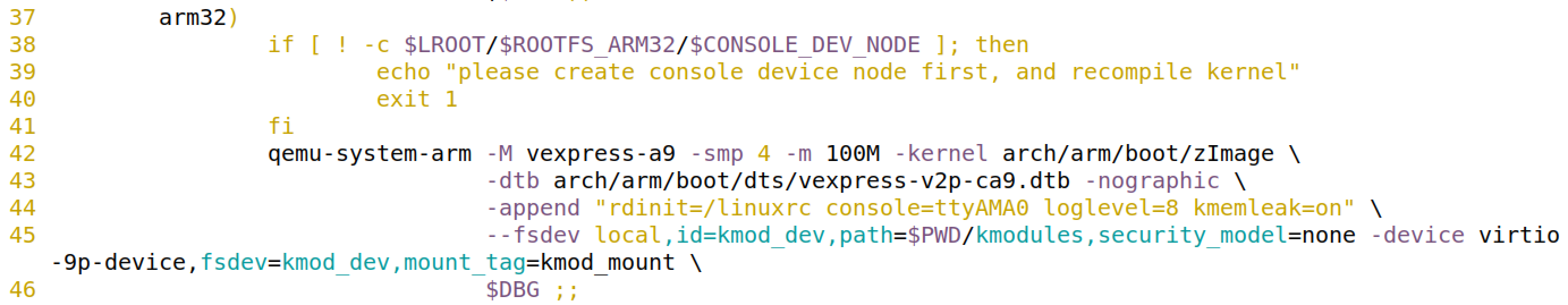
CONFIG\_DEBUG\_KMEMLEAK=y

CONFIG\_DEBUG\_KMEMLEAK\_DEFAULT\_OFF=y

CONFIG\_DEBUG\_KMEMLEAK\_EARLY\_LOG\_SIZE=4096

1. 重新编译内核。
2. 在内核commandline中添加“kmemleak=on”字符串来打开该功能。

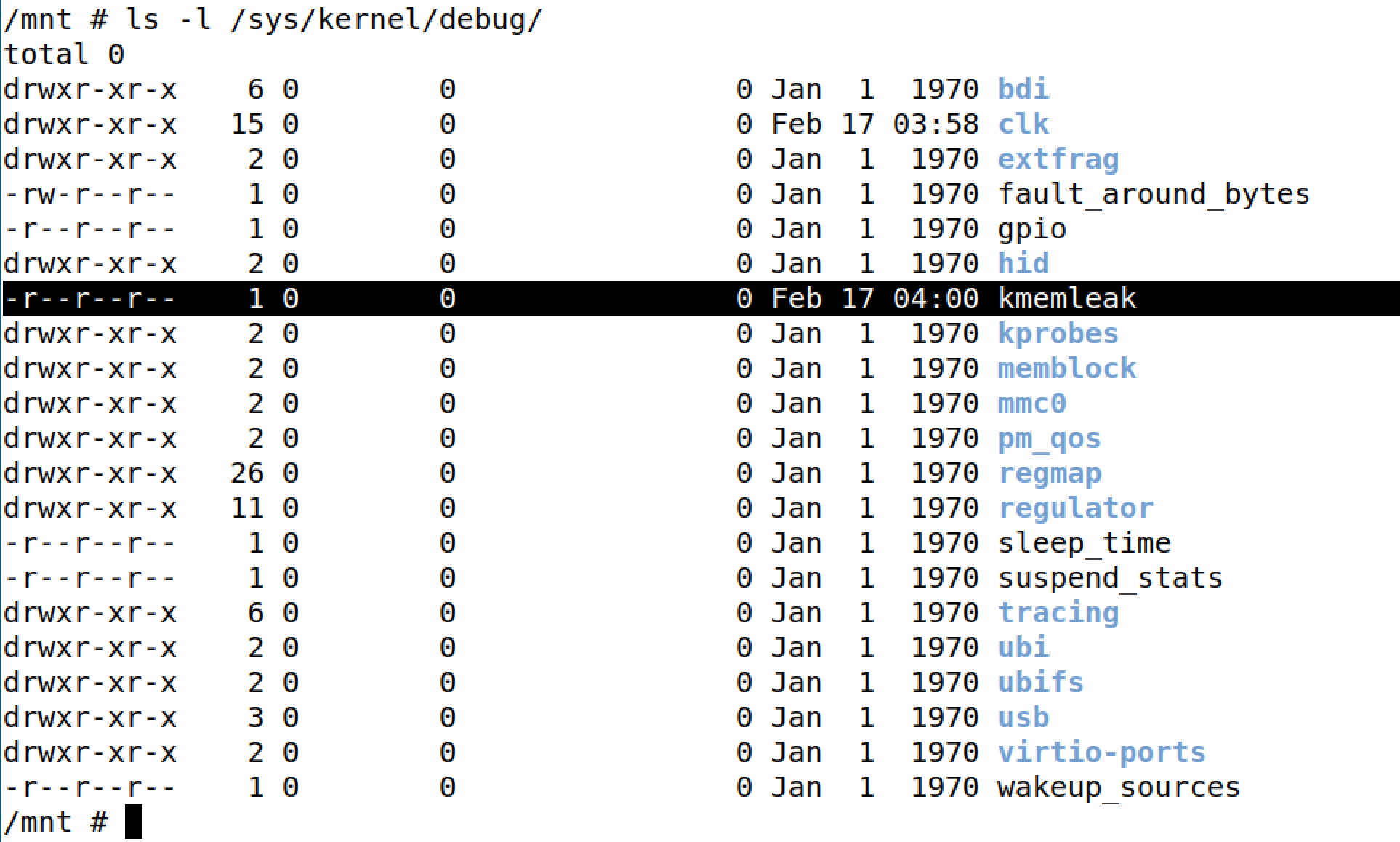
读者可以在run.sh这个脚本里添加了。



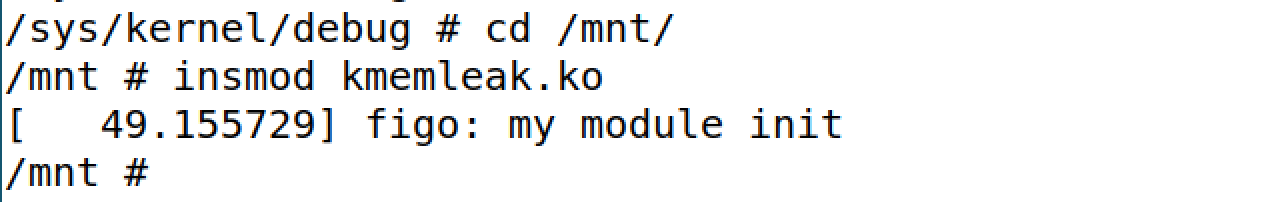
1. 编译kmemleak的测试内核模块。
2. 把内核模块拷贝到kmodules目录。
3. 运行Qemu虚拟机。

|  |
| --- |
| # sh run.sh arm32 |

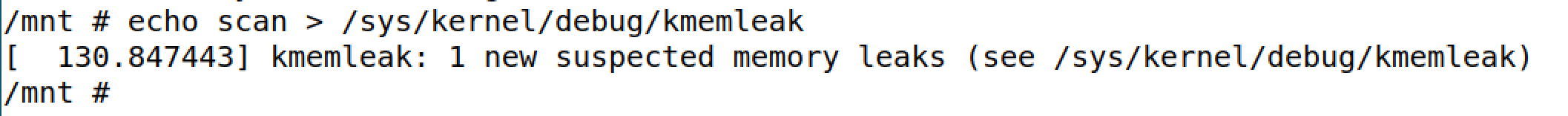
1. 检查kmemleak的debug节点有没有生成. Debug目录是在/sys/kernel/debug/.



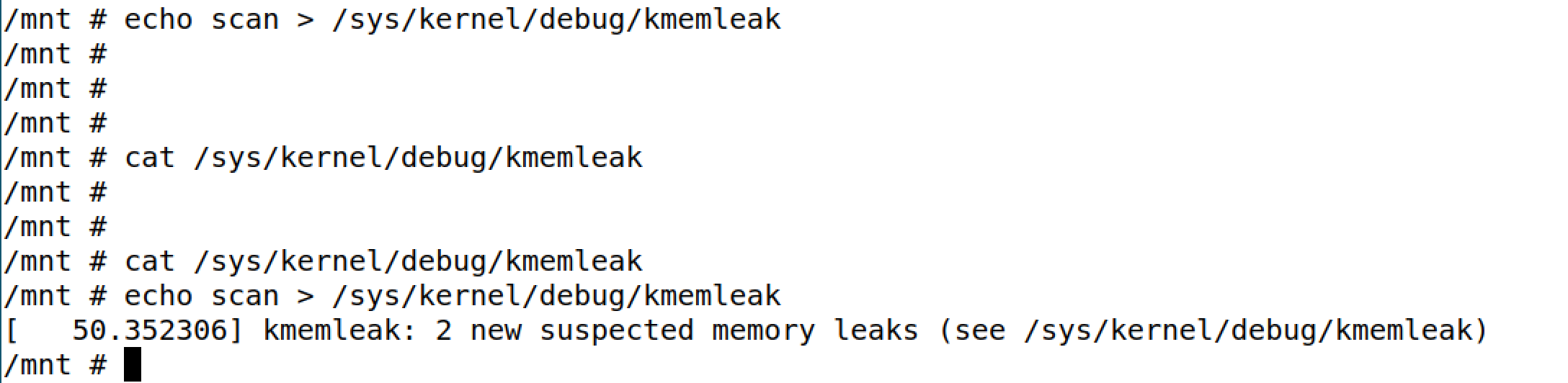
1. 进入mnt目录，运行测试内核模块。



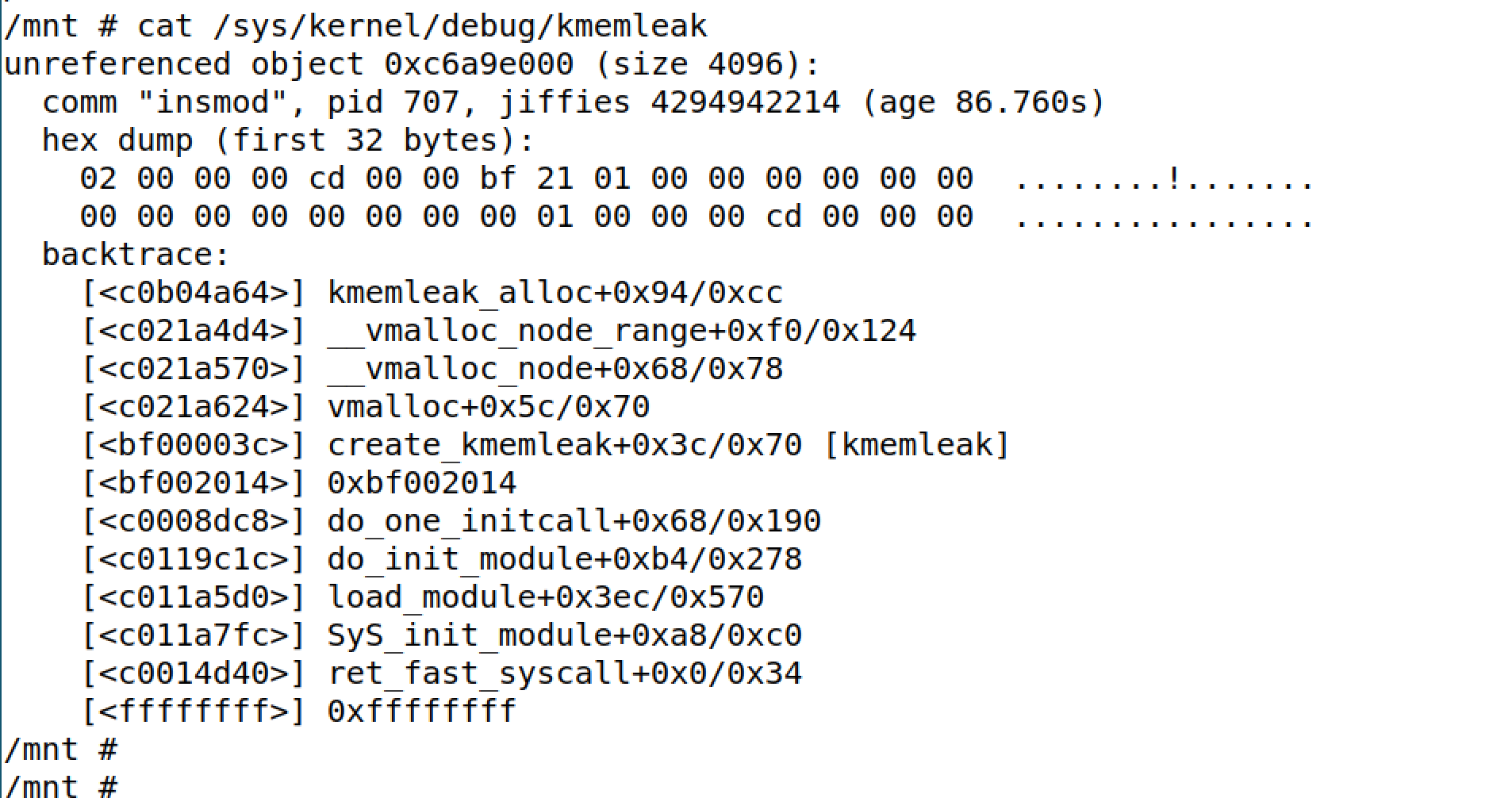
1. 向kmemleak写入scan命令开始扫描



如果没有发现可疑的内存泄漏, 可以尝试在一次scan.



发现了可疑的内存泄漏.



### 进阶思考

如果大家对这些问题感兴趣，可以关注笨叔的旗舰篇视频，笨叔会在视频中和大家详细解答。



订阅和购买旗舰篇视频可以到：

1. 微店：



1. 淘宝店：https://shop115683645.taobao.com/

微信公众号：

