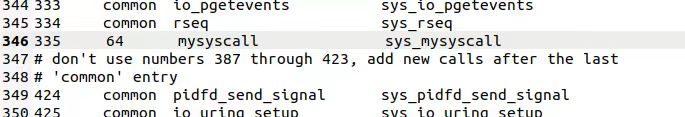
编译linux内核并加系统调用（遍历进程）

Linux版本 ubuntu-20.04.6

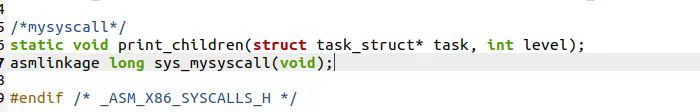
编译内核版本 5.10.216

更新系统调用表，添加系统调用id在arch/x86/entry/syscalls/syscall\_64.tbl



添加系统调用函数声明

修改arch/x86/include/asm/syscalls.h



在内核源代码添加函数定义 kernel/sys.c



安装编译所需工具

sudo apt-get install gcc make libncurses5-dev openssl libssl-dev

sudo apt-get install build-essential

sudo apt-get install pkg-config

sudo apt-get install libc6-dev

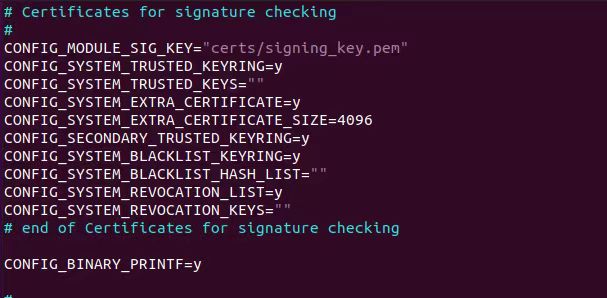
sudo apt-get install bison

sudo apt-get install flex

sudo apt-get install libelf-dev

make menuconfig 先默认操作 再修改config文件

修改结果如图



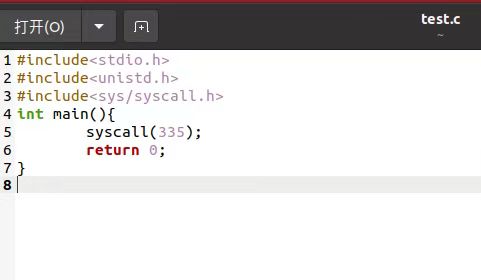
编译成功后 安装模块

sudo make modules\_install

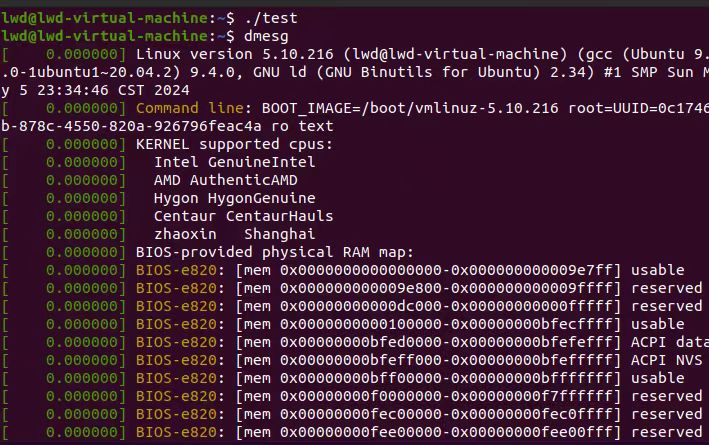
sudo make install

修改开机启动项 重新开机 切换内核

编写测试案例 调用新加的系统号335



检查结果



系统调用添加成功！

遇到的问题：

1.版本不匹配内核编译不通过 换用以前版本的内核重新编译

2 asmlinkage long sys\_mysyscall(void)在高版本的内核中很可能会出现以下报错：  
arch/x86/entry/syscall\_64.o:(.rodata+0xa78): undefined reference to '\_\_x64\_sys\_mysyscall'

更改为 SYSCALL\_DEFINE0(mysyscall)

3.编译中断后 需清理之前编译错误的无用文件 再重新编译 不然容易报错

4. 没有规则可制作目标“debian/canonical.certs.pem”  
make: \*\*\* [Makefile:1800:certs] 错误.2

修改：将.config文件中的CONFIG\_MODULE\_SIG\_ALL CONFIG\_MODUL CONFIG\_DEBUG\_INFO也注释掉