**操作系统课程实践（网安）**

# 实验1 Linux 内核编译及添加系统调用

## 实验介绍

本实验通过修改Linux内核源码，添加新的Linux系统调用，替换编译后内核，并测试结果，了解Linux内核源码的编译方法和内核的安装方法，系统调用的概念、编写步骤和调用方法。

## 任务描述

掌握Linux 系统调用基本概念

Linux 内核源码的编译和安装

添加Linux 的系统调用

Linux 的系统调用的测试方法

## 实验目的

学习掌握Linux内核的编译和启用

学习掌握如何添加Linux 的系统调用

学习掌握测试Linux系统调用

## 实验内容

1. 掌握Linux 内核的编译与安装【本实验也可采用tatakOS或者xv6来实现，见《实验 1：补充1》】

### 阅读教材7.2.4节Linux 内核编译步骤，网上查找资料，了解Linux内核编译的基本概念和步骤。

### 登录华为云，完成openEuler内核的编译与安装（也可以在VMWare虚拟机中完成x86-64位openEuler内核的编译与安装，参照下面步骤和网上资料做相应修改）。

### 登录系统并查看当前内核版本

[root@openEuler ~]# uname -r

4.19.???

### 安装工具，构建开发环境：

[root@openEuler ~]# yum group install -y "Development Tools" –nogpgcheck

（如果遇到安装时提示xxx not signed, GPG check Failed等错误，尝试加入“--nogpgcheck”，比如 yum group install -y "Development Tools" --nogpgcheck）

[root@openEuler ~]# yum install -y bc

[root@openEuler ~]# yum install -y openssl-devel

### 备份boot目录以防后续步骤更新内核失败

[root@openEuler ~]# tar czvf boot.origin.tgz /boot/

保存当前内核版本信息

[root@openEuler ~]# uname –r > uname\_r.log

### 获取内核源代码并解压

[root@openEuler ~]# wget <https://gitee.com/openeuler/kernel/repository/archive/kernel-4.19.zip> (UPDATE 链接已经失效，改在这里<https://gitee.com/openeuler/kernel/releases下载最新版本，比如2023-03-29>发布的 <https://gitee.com/openeuler/kernel/archive/refs/tags/4.19.90-2303.5.0.zip> ，可以在本机上下载后上传到云服务器)

[root@openEuler ~]# unzip kernel-4.19.zip

### 编译内核

[root@openEuler ~]# cd kernel

[root@openEuler kernel]# make openeuler\_defconfig

在这里，我们按源代码文件kernel/arch/arm64/configs/openeuler\_defconfig的配置配置内核，此外，建议大家可以试试make menuconfig，看一下编译内核有哪些可配置项（<https://blog.csdn.net/howiexue/article/details/76696631>）。

[root@openEuler kernel]# make help | grep Image

\* Image.gz - Compressed kernel image (arch/arm64/boot/Image.gz)

Image - Uncompressed kernel image (arch/arm64/boot/Image)

这一步查看了可编译的Image。

[root@openEuler kernel]# make -j4 Image modules dtbs

这一步是编译内核的Image、modules和dtbs，make -j 4表示4个线程编译（可以根据CPU核数调整）

### 安装内核

[root@openEuler kernel]# make modules\_install

……

INSTALL sound/soundcore.ko

DEPMOD 4.19.154

[root@openEuler kernel]# make install

/bin/sh ./arch/arm64/boot/install.sh 4.19.154 \

arch/arm64/boot/Image System.map "/boot"

dracut-install: Failed to find module 'xen-blkfront'

dracut: FAILED: /usr/lib/dracut/dracut-install -D /var/tmp/dracut.tlIdPu/initramfs --kerneldir /lib/modules/4.19.154/ -m virtio\_gpu xen-blkfront xen-netfront virtio\_blk virtio\_scsi virtio\_net virtio\_pci virtio\_ring virtio

注意：在最后一步“make install”时出现的错误在这里可以忽略。

### 以VNC登录ECS



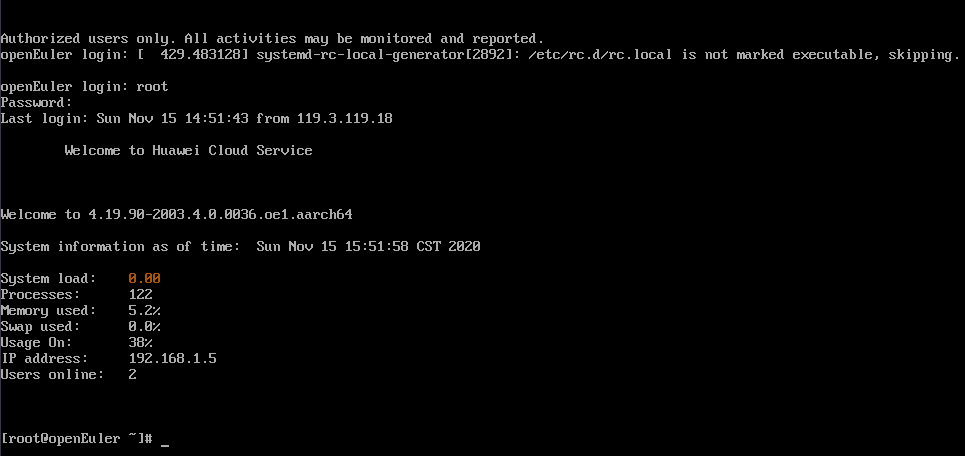
在控制台“弹性云服务器ECS”的页面中点击刚刚创建的虚拟机“openEuler”的名字超链接，在新打开的页面中点击“远程登录”按钮：



然后以控制台提供的VNC方式登录：



与以ssh登录一样，以root身份登录：



大部分的时间，我们仅将此作为一个监视器使用。

### 重启系统

在ssh终端重启操作系统：

[root@openEuler kernel]# reboot

### 登录并验证

在VNC窗口中选择以新编译出来的内核启动系统：



在这里新编译出来的内核版本为4.19.154。您的子版本号可能与此不一样。

### 登录系统并查看版本

请以VNC和/或ssh终端登录系统，并在其中查看内核版本：

[root@openEuler ~]# uname -r

4.19.154

可以看出内核版本已更新。

1. 掌握Linux 系统调用基本概念

### 阅读教材7.2.2节Linux 系统调用基本概念，掌握Linux系统调用的基本概念。

### 通过网站http://lxr.free-electrons.com，查看你所安装的openEuler操作系统内核版本源码和系统调用相关的部分，对比x86\_64和arm64系统相关文件的区别。

### 学习Linux内核API，可以参考《LINUX内核API完全参考手册》，Linux内核文档<https://www.kernel.org/doc/html/latest/>，Linux内核源码，了解下列内核API函数的功能和使用方法。

* [**printk**](https://www.kernel.org/doc/html/latest/core-api/printk-basics.html)**（https://www.kernel.org/doc/html/latest/core-api/printk-basics.html）**
* **copy\_to\_user, copy\_from\_user**
* **find\_get\_pid,pid\_task,task\_nice,task\_prio,set\_user\_nice**

### 阅读教材7.2.3节Linux 添加系统调用的步骤，添加一个新的系统调用，通过内核打印调试语句printk打印自己的学号。(<https://www.kernel.org/doc/html/v4.10/process/adding-syscalls.html>)

1. 设计和添加Linux 系统调用

### 请从下面给出的系统调用题目中，选择2个题目（其中第1个题目为必做），设计系统调用的函数名、参数和返回值，并完成系统调用的实现，添加和测试。

### 修改或返回指定进程的优先级（nice值和prio值）（详见教材P328）

### 提示：可能参考的内核函数：set\_user\_nice()

### 返回指定进程的内存管理信息，如进程可执行代码的起始及结束地址、已初始化数据的起始及结束地址、用户态堆栈起始地址、堆起始地址等。

### 提示：可能参考的内核函数：get\_task\_mm()

### 返回指定进程当前的状态、各种用户信息，并能解释说明各种用户的含义、所使用的Linux内核版本中进程状态的设置情况。

### 返回指定进程的各种调度相关信息，比如各种优先级、采用的调度策略、运行该进程的CPU编号、进程的剩余时间片长度等，能解释各种优先级的含义。

### 返回当前系统的名称和版本

### 提示：可能参考的内核函数：version\_proc\_show()

### 参考文献：https://blog.csdn.net/u012010054/article/details/87714168

### 输出一个指定文件的相关信息，如索引节点编号、硬连接数、文件所有者标识符、文件的字节数和访问方式等。

### 返回指定进程的相关时间信息，如进程创建时间、进程在用户态及内核态的运行时间、进程的所有子孙进程在用户态的运行时间及在内核态的运行时间等。

### 返回当前进程的pid和父进程的pid

### 改变主机名称为自定义字符串

### 提示：参考/etc/hostname文件内容

### 把指定文件变为长度为0的空文件

### 让系统倒计时指定秒数后重启

### 提示：可能会用到reboot()函数或者kernel\_restart()。

### 返回指定进程当前的状态、各种用户信息，并能解释说明各种用户的含义、所使用的Linux内核版本中进程状态的设置情况。

### 把源文件2的内容插入到源文件1的前面

### 获取指定进程标识符PID所对应的资源使用情况，包括用户态和内核态的执行时间（以秒和微秒为单位）、无需和需要物理输入输出操作的页面错误次数、进程置换出内存的次数。（参考getrusage和sys\_getrusage）

### 返回指定文件的相关信息，如索引节点编号、硬连接数、文件所有者标识符、文件的字节数和访问方式等。