QEMU环境搭建

下载Linux内核代码

在终端内输入指令

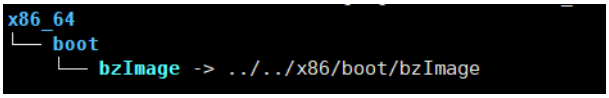
```
git clone -b staging-testing git://git.kernel.org/pub/scm/linux/kernel/git/gregkh/staging.git
```

下载linux-6.16.0内核源码，之后配置并编译内核

```
cd staging # cd linux-6.16.0
make x86_64_defconfig
make menuconfig
```

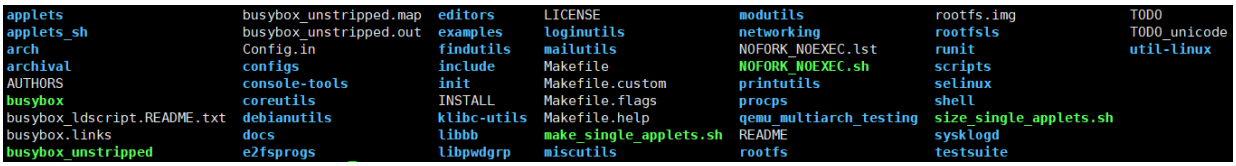
输入对应指令进入配置菜单，启用内核debug，关闭地址随机化，不然断点处无法停止。之后开始编译内核使用`make -j 12`进行编译。

编译完成后在arch/x86_64/boot/bzImage中会出现对应的内核文件bzImage如下图所示：



配置Busybox

下载Busybox并解压其文件夹内容如图所示：



将配置设置为静态编译后`make -j 12`进行编译

制作rootfs

接下来制作rootfs镜像文件，并把busybox安装到其中。 使用dd命令创建文件，并格式化为ext4文件系统。使用代码：

```
dd if=/dev/zero of=rootfs.img bs=1M count=512
mkfs.ext4 rootfs.img
```

创建用于挂载该镜像文件的目录 `rootfs`，使用 `mount` 命令将 `rootfs.img` 挂载到`rootfs`目录，编译 busybox 并写入`rootfs` 目录中。

```
mkdir rootfs
sudo mount -t ext4 -o loop rootfs.img ./rootfs
sudo make install CONFIG_PREFIX=./rootfs
```

对写入的busybox进行补充配置。

```
cd rootfs/
sudo mkdir proc dev etc home mnt
sudo cp -r ../examples/bootfloppy/etc/* etc/
```

最后，卸载rootfs.img

```
cd ..
sudo umount rootfs
```

至此，一个带有rootfs的磁盘镜像制作完成。

启动QEMU

使用如下命令启动无GUI的qemu：

```
qemu-system-x86_64 -kernel ./staging/arch/x86_64/boot/bzImage -hda=./disk/rootfs.img -append "root=/dev/sda console=ttyS0" -nographic
```

启动完成后使用`uname -a`查看内核版本如图所示：

```
~ # uname -a
Linux (none) 6.16.0-11568-gd632ab86aff2 #2 SMP PREEMPT_DYNAMIC Thu Aug  7 18:52:57 CST 2025 x86_64 GNU/Linux
```