GDB+Qemu调试Linux-0.11的代码

笔记本:	内核
创建时间:	2020/10/24 15:01
作者:	243319818
URL:	https://www.jianshu.com/p/ab4fa7f12f06

GDB+Qemu调试Linux-0.11的代码

readilen

0.066 2019.08.18 23:34:13 字数 254 阅读 795

1.下载内核源码和根文件系统镜像
http://oldlinux.org/Linux.old/bochs/linux-0.11-devel-040809.zip

Linux-0.11内核源码的改进版，可以在gcc- 5.5.0下顺利编译通过，原生代码只能在gcc-1.4下编译：
https://github.com/yuanxinyu/Linux-0.11

2.编译Linux-0.11
解压Linux-0.11-master.zip，进入Linux-0.11-master目录中，直接执行make就可以编译内核

会生成2个文件，一个是内核Image， 一个是内核符号文件tools/system。

3.qemu启动虚拟机
提取出linux-0.11-devel-040809.zip中的hdc-0.11.img，
按下面命令执行：

```
qemu-system-x86_64 -m 16 -boot a -fda Image -hda hdc-0.11.img -s -S
```

解释一下

```
-fda Image：代表你把 Image 執行目錄下

-hda hdc-0.11.img：代表你把 HD img，是一个模拟硬盘的文件，可以在赵博士所提供的`linux-0.11-devel-040809.zip`找到

-m：设定模拟的内存大小，本地设定为 16MB

-s ：服务器开启1234端口

-S：开始执行就挂住
```

另外开启控制台

```
gdb tools/system
```

进入客户端
载入符号

```
(gdb) file tools/system
```

链接远端服务器

```
(gdb) target remote localhost:1234
```

```
(gdb) target remote localhost:1234
```

下中断，停在0x7c00处

```
(gdb)target remote localhost:1234   //连接gdbserer
(gdb)directory ./Linux-0.11-master  //设置源码目录
(gdb)set architecture i8086 //设置成i8086模式，用来调试16位实模式代码
(gdb)set disassembly-flavor intel    //讲汇编显示成INTEL格式，好看一些
(gdb)b *0x7c00  //在地址0x7c00处打断点，因为系统加电后，BIOS会把MBR中的代码加载到内     存中的0x7c00的位置，并从0x7c00处开始执行bootsect.s的代码
(gdb)  layout split
(gdb)  c
```

在此時，bios 把控制权正式的交给了 linux,而 0x7C00对应的代码应该是 bootsect.S
观察0x7DFE与 0x7DFF的值是否为0x55，0xAA

```
(gdb) x/16xb 0x7DF0
```

单步执行

```
(gdb) si
```

下中断

```
(gdb) b main
```


readilen 关注人工智能，量化投资，深度学习，自然语言，视觉图形，Web前端 微信公众号：PyT...
总资产243 (约16.74元)　共写了32.1W字　获得900个赞　共1,512个粉丝