

## gdb 调试 UML (user mode linux)

UML (user mode linux): 将 linux 当做应用层的进程, 所以可以用 gdb 调试。

Step1: 默认配置: `make defconfig ARCH=um`

Step2: 选择相关配置: `make menuconfig ARCH=um`

选择:

- Kernel hacking->Kernel debugging
- Kernel hacking->Compile-time checks and compiler options->Compile the kernel with debug info
- Kernel hacking->compile-time checks and compiler options->Compile the kernel with frame pointers

Step3: `make ARCH=um -j (内核数*2)`

编译成功之后, 在源码的根目录下有 `linux` 和 `uml` 可执行文件。

Step4: 文件系统。现在已经编译好了 um 的内核, 但是没有文件系统。下载文件系统: <http://fs.devloop.org.uk>, 下载文件系统。解压到编译好的源码的目录下。如 `bunzip2 Debian-Wheezy-AMD64-root_fs.bz2`。

Step5: 制作 swap 文件系统, 主要作用是使 UML 运行更加稳定。(可选)

```
dd if=/dev/zero of=swap_fs bs=1M count=512
```

```
sudo mkswap swap_fs
```

Step6: 启动 UML。但必须是超级用户 root。先进入已编译好的源码目录下。

```
Sudo bash
```

```
./linux ubda=Debian-Wheezy-AMD64-root_fs ubdb=swap_fs mem=256M
```

(注: ubda: 根文件 ubdb: 交互文件 mem: UML 内存)

当成功启动 UML, 会有这样的界面:

```
Serial line 0 assigned device '/dev/pts/5'
Debian GNU/Linux 7 changeme tty0

changeme login: root
Last login: Thu Apr 14 12:36:50 UTC 2016 on tty0
Linux changeme 3.15.0 #1 Thu Apr 14 16:39:26 CST 2016 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@changeme:~#
```

第一次的登陆只能是 root。

Step7: 寻找 UML 的进程号，另开一个终端。输入 `ps -el | grep linux`。如下

```
koala@koala:~/linux-3.15$ ps -el | grep 'linux'
4 S    0 26825 26824 4 80 0 - 69217 - pts/4 00:00:04 linux
1 S    0 26832 26825 0 80 0 - 69217 - pts/4 00:00:00 linux
1 S    0 26833 26825 0 80 0 - 69217 - pts/4 00:00:00 linux
1 S    0 26834 26825 0 80 0 - 69217 - pts/4 00:00:00 linux
1 t    0 26835 26825 0 80 0 - 4054 - pts/4 00:00:00 linux
1 t    0 27024 26825 0 80 0 - 4197 - pts/4 00:00:00 linux
1 t    0 27114 26825 0 80 0 - 3851 - pts/4 00:00:00 linux
1 t    0 27115 26825 0 80 0 - 3852 - pts/4 00:00:00 linux
1 t    0 29178 26825 0 80 0 - 4376 - pts/4 00:00:00 linux
1 t    0 29249 26825 0 80 0 - 3860 - pts/4 00:00:00 linux
1 t    0 29302 26825 0 80 0 - 3855 - pts/4 00:00:00 linux
1 t    0 29304 26825 0 80 0 - 4242 - pts/4 00:00:00 linux
1 t    0 29306 26825 0 80 0 - 4425 - pts/4 00:00:00 linux
koala@koala:~/linux-3.15$
```

图中每一行，第 4 个参数为第 5 个参数的子进程。  
图中处理第一行之外的每一行，都显示进程号为 26825 的进程是其他进程的父进程。因此 PID=26825 的进程是 UML 进程。

Step8: 启动 gdb。另打开一个终端。输入 `gdb ./linux`

Step9: 退出 UML。切换到 UML 的终端。输入 `init 0`，即可退出。

参考:

<http://user-mode-linux.sourceforge.net>

<http://user-mode-linux.sourceforge.net/source.html>

<http://user-mode-linux.sourceforge.net/configure.html>