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

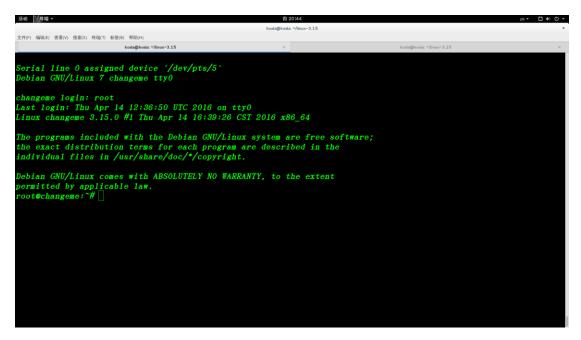
Step3: make ARCH=um -j (内核数*2) 编译成功之后,在源码的根目录下有 linux 和 vmlinux 可执行文件。

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: udba: 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:



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

														0:26 ~/linux=3.15		zh *	
E) 184	B(F) 3	悪心	n system n	#	を端(T) 标签(B) \$50	VH)						коацашкоаца	-/unux-3.15			
	4(-) =		*/ 13CM((3)		CHE(1) 1973E1				ux-3.1	5			×			koala@koala: ~/linux~3.15	
0.1.07	nle o	. 1	~ · ~ /:	,	nux-3				-e1		anon.	'linux				nessagement junes size	
91 4 0					пих-з 26824	. 100	у р 8				69217		pts/4	00:00:04	1.1		
3					26825	0	8				69217		pts/4 pts/4	00:00:04			
3					26825	0	8				69217		pts/4	00:00:00			
					26825 26825	0	8				69217		pts/4 pts/4	00:00:00			
3					26825 26825	0	8						pts/4 pts/4	00:00:00			
					26825	0	8						pts/4	00:00:00			
					26825	0	8				3851		pts/4	00:00:00			
					26825	0	8				3852		pts/4	00:00:00			
					26825	0	8						pts/4	00:00:00			
					26825	0	8						pts/4	00:00:00			
					26825	0	8				3855		pts/4	00:00:00			
					26825	0	8						pts/4	00:00:00			
t _					26825		. 8	0	0		4425		pts/4	00:00:00	linux		
ıla(D ko 8	11	a:~/]	li.	nux-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。



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