Lab3: Kernel Debugging

杨润东 10205102454[at]stu.ecnu.edu.cn

- 什么是调试
- 用GDB直接调试
- 用IDE[VSCode(迫真IDE)]调试

什么是调试

一杯茶，一包烟，一个bug调一天。

灵魂提问：什么是调试？

> In computer programming and software development, **debugging** is the process of finding and resolving *bugs* (defects or problems that prevent correct operation) within computer programs, software, or systems.
> Debugging tactics can involve interactive debugging, control flow analysis, unit testing, integration testing, log file analysis, monitoring at the application or system level, memory dumps, and profiling. Many programming languages and software development tools also offer programs to aid in debugging, known as ***debuggers***.
> ——*Debugging - Wikipedia*

- TLDR：修bug。

什么是调试

一杯茶，一包烟，一个bug调一天。

我们所说的调试：

用GDB直接调试

一杯茶，一包烟，一个bug调一天。

我们已经讲过GDB的简单使用：

- r/b/c/n/s/p... 基本上够用了

而作为神通广大的GNU Debugger，肯定是有其它复杂但有用的拓展功能的。在gdb命令行执行`help all`就可以看到所有gdb commands了。

- 很多神奇的功能，但大部分大概率用不到。
- 一部分可以帮助我们调试xv6。

用GDB直接调试

一杯茶，一包烟，一个bug调一天。

GDB原理简单介绍：

1. `gcc example.c -g -o example` 编译时加载调试信息（这是什么？）

   > DWARF - Wikipedia

2. `gdb example` 用gdb的各种commands调试`example`程序（发生了什么？）

   > 1. `fork() exec()`来执行`example`
   > 2. `ptrace()`
   >   - provides a means by which one process may observe and control the execution of another process.

- 如何远程调试？

  > GDB Remote Serial Protocol

用GDB直接调试

一杯茶，一包烟，一个bug调一天。

- `$ make qemu-gdb` or `$ make qemu-nox-gdb`
- 打开一个gdb，`target remote dest_ip `
- 成功连接后就会自动开始，然后就和本地调试一模一样了

> .gdbinit可以帮助你快速配置gdb环境
> gdbinit(5) - Linux manual page (man7.org)

用IDE[VSCode(迫真IDE)]调试

还得是GUI

- 其实IDE也是用debugger调试，只不过是把过程和结果都可视化了
- launch.json

  > 所谓的“配置vscode”

- 不光能调内核!
- xv6也有自己的调试方法

> 具体参见xv6Debug.pdf