

PA 2-2 实验报告

221220085 时昌军

一、实验目的

在上一节中所展开的实现指令的实验中，测试用例的可执行目标文件是通过交叉编译并使用 `objcopy` 直接得到对应的内存镜像加载到内存中执行的。在真实的计算机系统中，这是一种效率极低的存储可执行文件的方法。现代类UNIX操作系统，如Linux，主要使用可执行可链接格式（Executable and Linkable Format，简称ELF）来存储目标文件。本节我们就目标文件的装载展开讨论。

二、实验过程

1. 修改 `testcase/Makefile` 中 `LDFLAGS` 并 `make clean`
2. 实现Kernel中的 `loader()`；
3. 使用 `make test_pa-2-2` 执行测试用例并通过。

三、实验心得

pa2-2 的难度不大，代码实现较简单，主要收获是学习了elf文件的格式和装载以及NEMU的kernel，为接下来的阶段做好准备。

四、思考题

1. 为什么在装载时要把内存中剩余的 `p_memsz - p_filesz` 字节的内容清零？

答：这块内容是当前使用不到的空余部分，将该部分清零可以防止上次装载的内容占据这部分空间，在程序运行过程中错误访问到这部分内容，从而发生不可预知的错误。