《软件安全》实验报告

姓名：张丛 学号：2113662 班级：信安一班

**实验名称：**

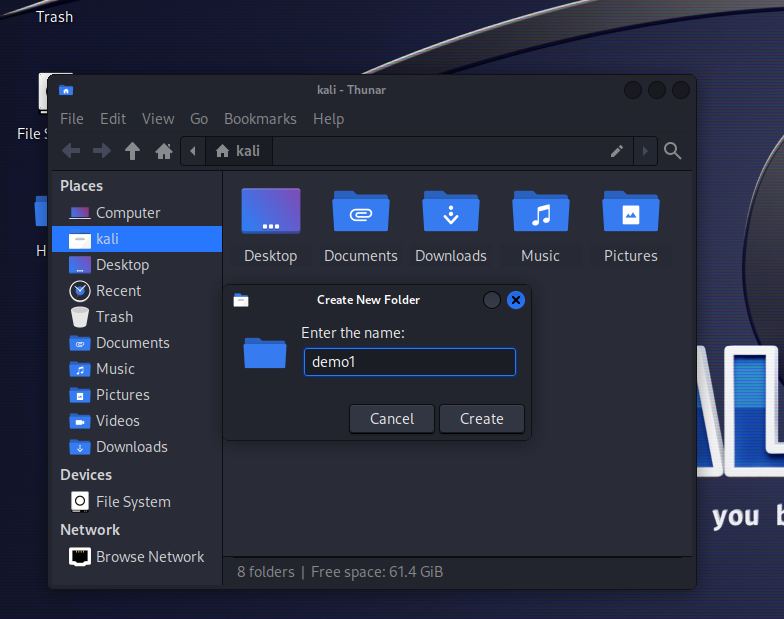
ALF模糊测试实验

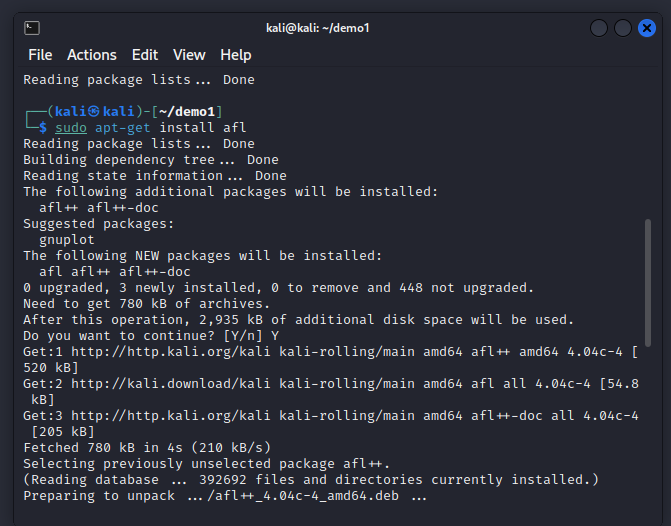
**实验要求：**

根据课本7.4.5章节，复现AFL在KALI下的安装、应用，查阅资料理解覆盖引导和文件变异的概念和含义

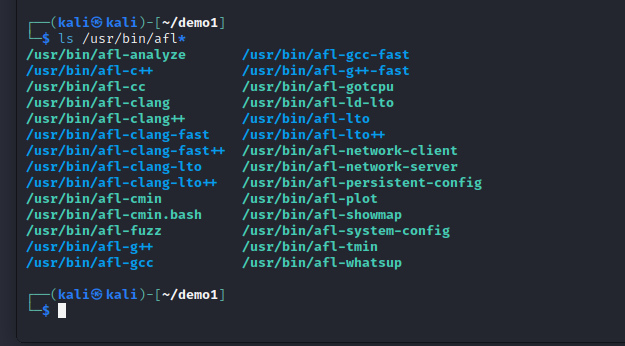
**实验过程：**

1. 进入Kali虚拟机，创建文件夹demo1,启动控制台，安装ALF

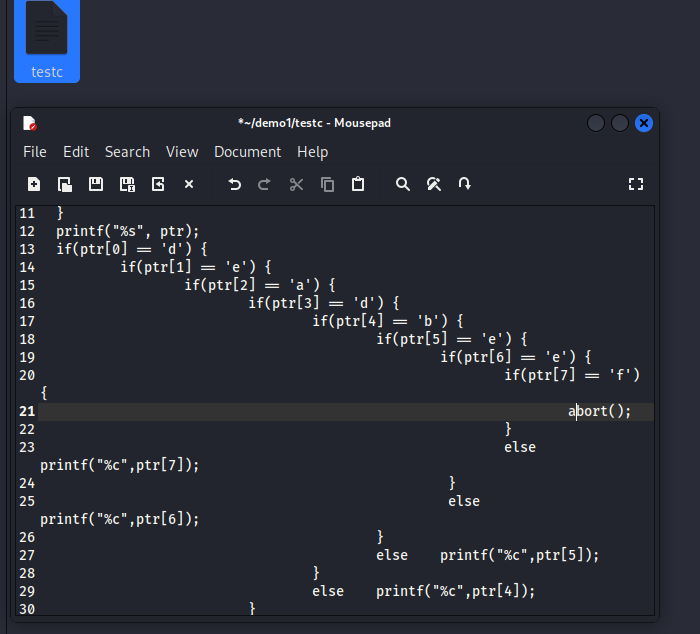




从安装目录查看AFL的功能支持：



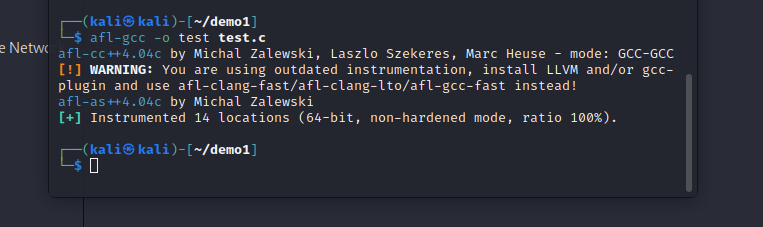
1. 新建test.c文档，复制案例程序



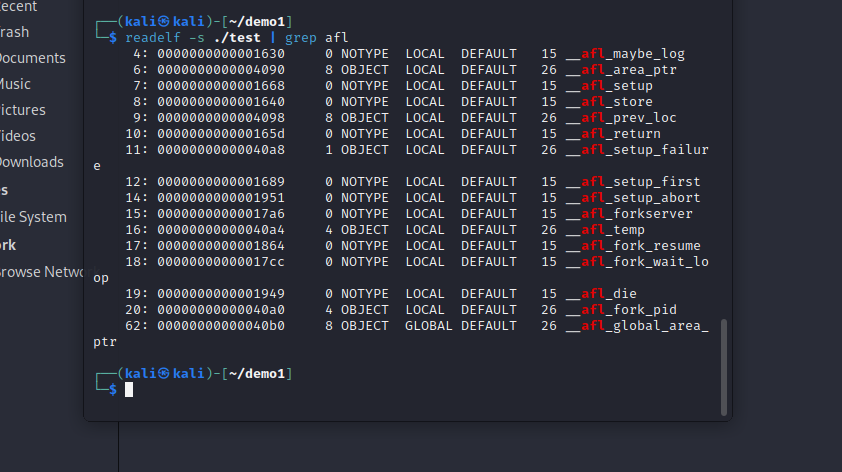
由程序可知：当输入deadbeef时会发生中断。

实验目标就是利用AFl找到这个漏洞。

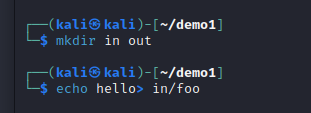
1. 编译运行，产生test可执行文件

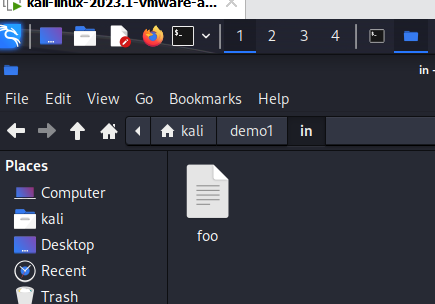


查看插桩：

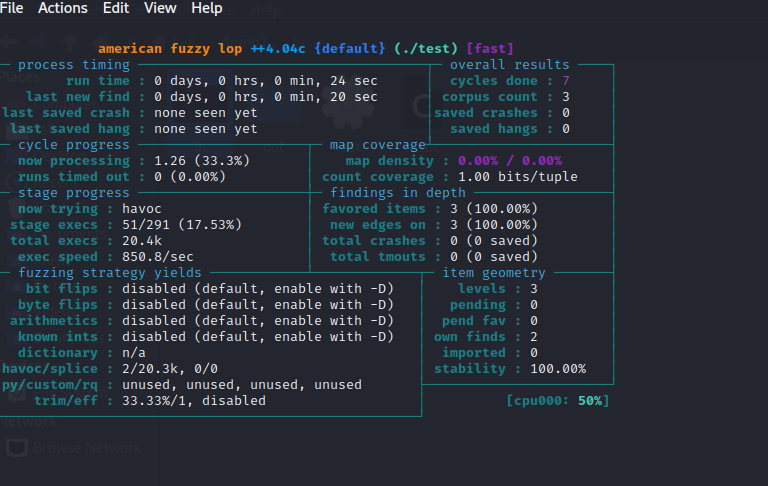


1. 创建输入输出文件、过程文件，开始测试

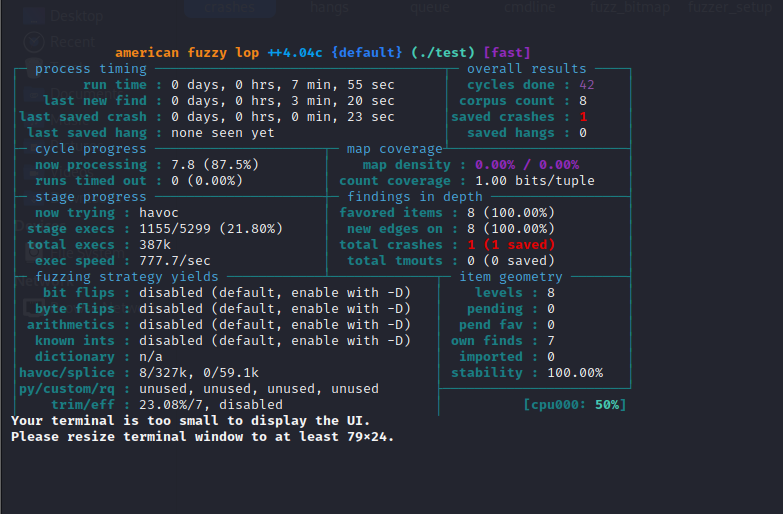




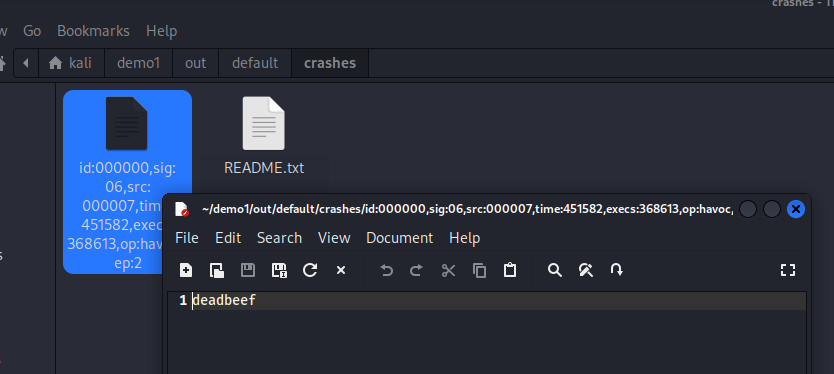
测试过程：



测试结果：



crashes文件结果：



可见，输入为deadfbeef时产生中断，即AFL检测到了漏洞。

**心得体会：**

通过实验，熟悉了AFL测试的过程，了解了AFL的功能。

学习到更多安全知识。

覆盖引导：即通过向目标程序插桩，统计代码覆盖，反馈给模糊测试引擎（即模糊测试工具），反馈信息用于变异种子，生成更高质量的输入，使得引擎能够用更好的输入让被测程序达到更高的代码覆盖率。

AFL是一款基于覆盖引导的模糊测试工具：通过记录输入样本的代码覆盖率，不断对输入进行变异，从而达到更高的代码覆盖率。

AFL 采用新型的编译时插桩和遗传算法自动发现新的测试用例，这些用例会触发目标二进制文件中的新内部状态。这大大改善了模糊测试的代码覆盖范围。