《漏洞利用及渗透测试基础》实验报告

姓名：沙璇 学号：1911562 班级：信息安全

**实验名称：**

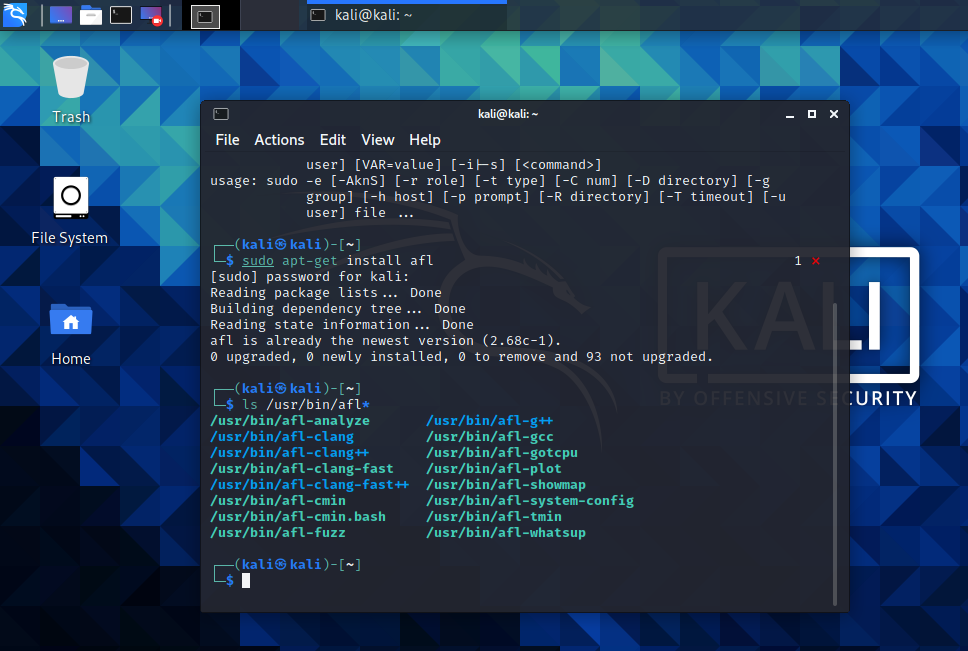
AFL模糊测试实验

**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.复现afl在kali下的安装，如下图：



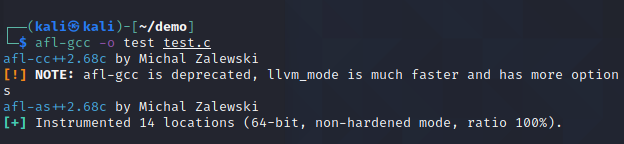
复现成功

2.复现afl的应用：

*①创建程序：*

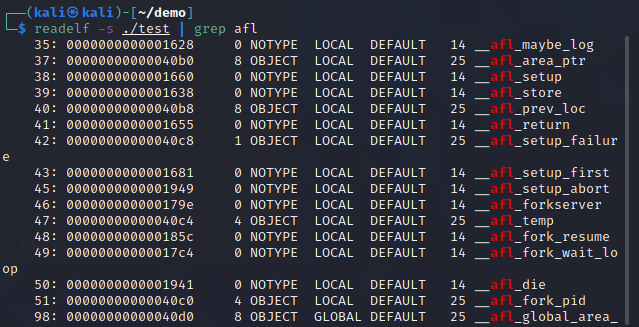
使用 afl 的编译器编译，可以使模糊测试过程更加高效。

命令：afl-gcc -o test test.c



编译后会有插桩（详见第 8.2 章）符号，使用下面的命令可以验证这一点。

命令：readelf -s ./test | grep afl



进行下一步之前，还需要输入如下命令指示系统将 coredumps 输出为文件，而不是将它们发送到特定的崩溃处理程序应用程序。

命令：echo core > /proc/sys/kernel/core\_pattern



*②创建测试用例*

命令：mkdir in out

然后，在输入文件夹中创建一个包含字符串“hello”的文件。

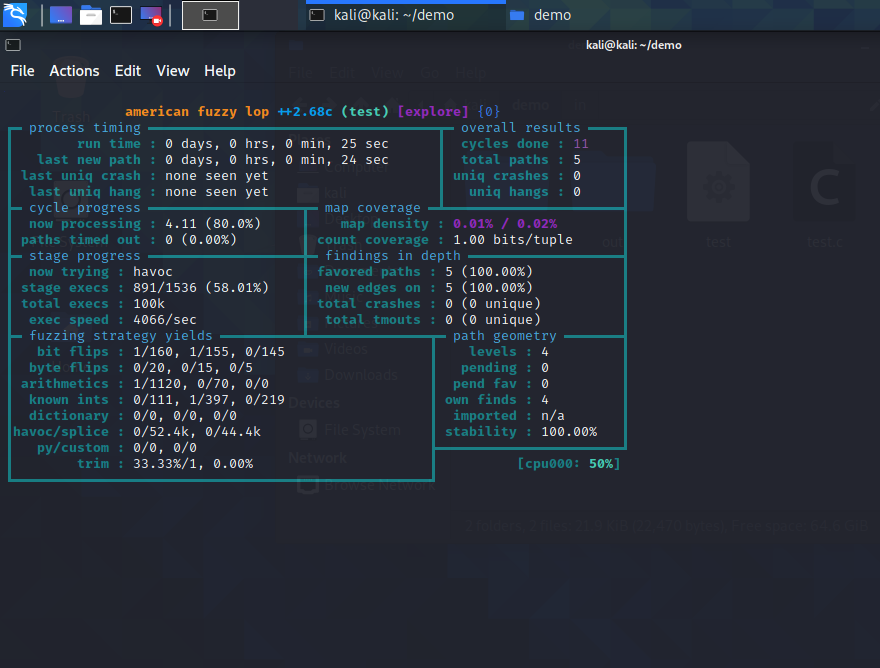
命令：echo hello> in/foo foo

就是我们的测试用例，里面包含初步字符串 hello。

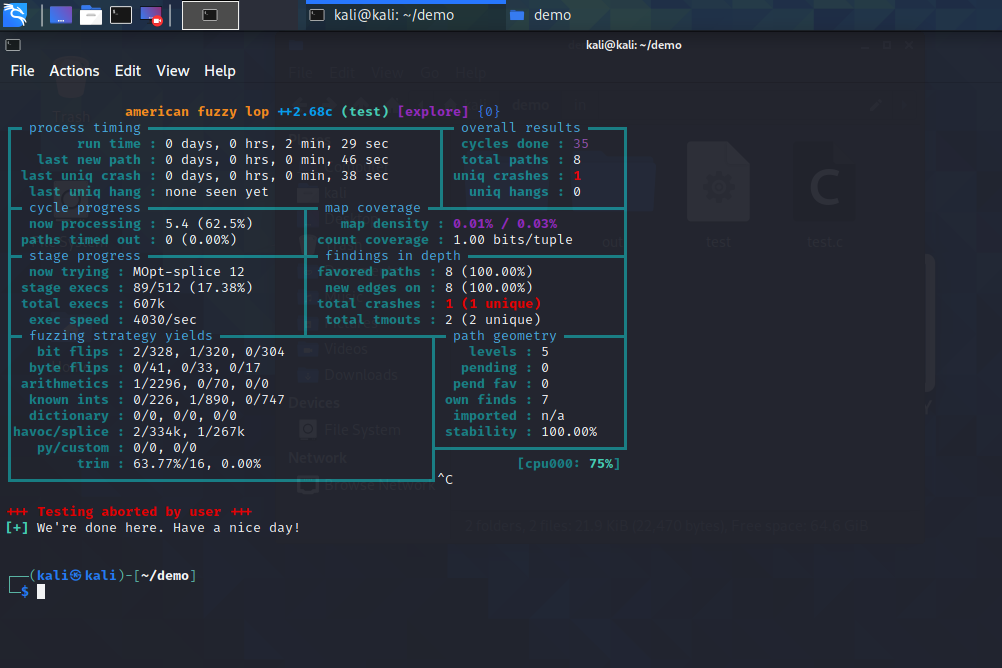
*③启动模糊测试*

运行如下命令，开始启动模糊测试：

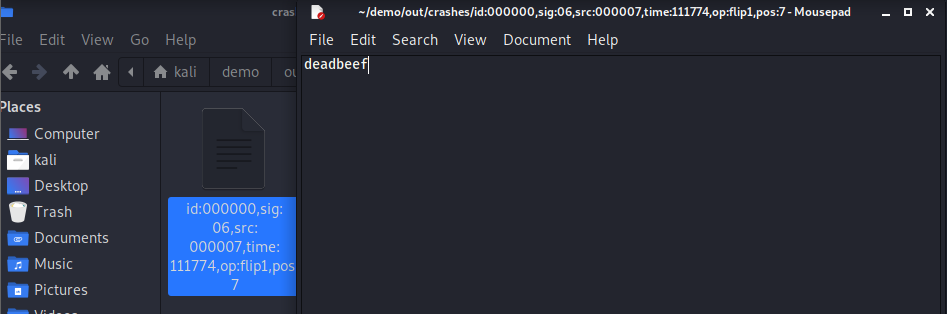
命令：afl-fuzz -i in -o out -- ./test @@

*④分析 crash*

观察 fuzzing 结果，如有 crash，定位问题。



在 out 文件夹下的 crashes 子文件夹里面是我们产生 crash 的样例：



**心得体会：**AFL 模糊测试框架功能非常强 大、非常有用