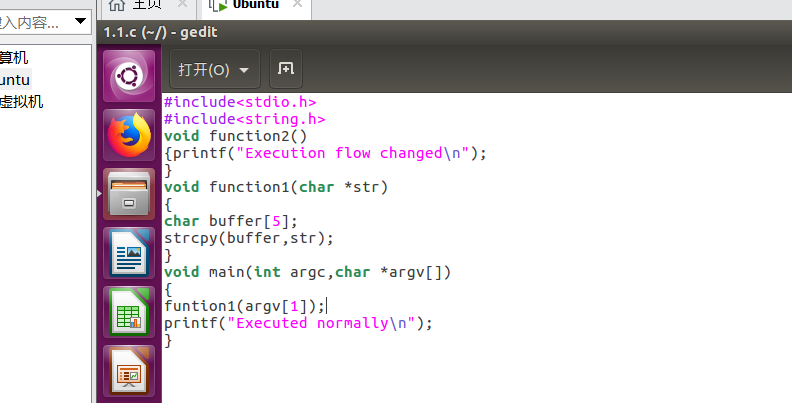
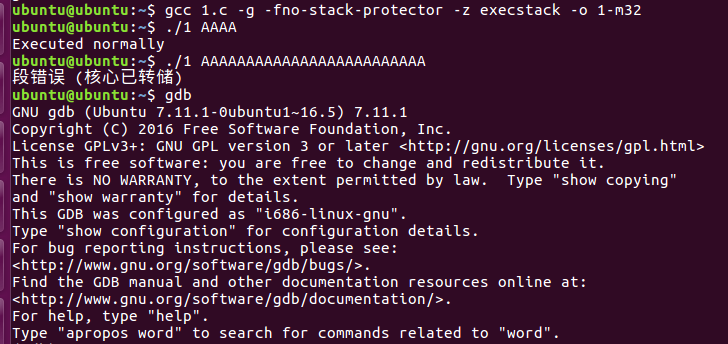
编写C语言

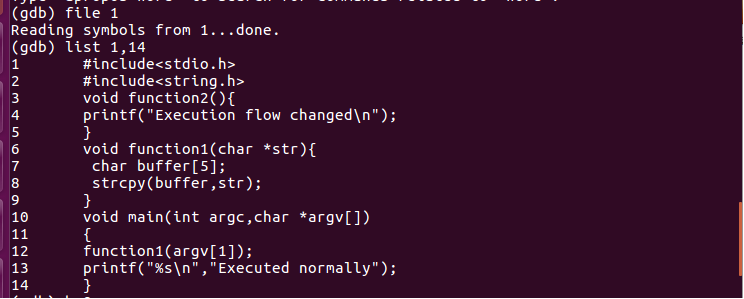


分别运行AAAA和AAAAAAAAAAAAAAAA

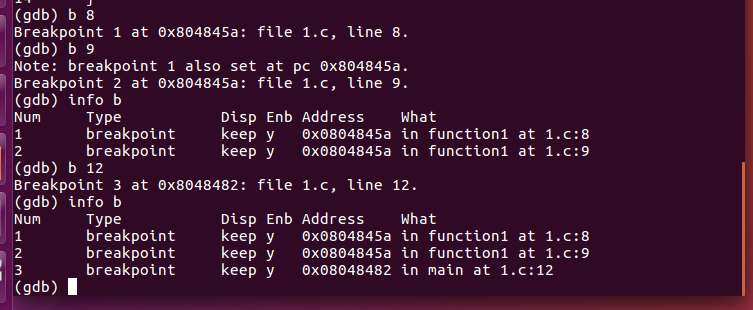


进入gdb

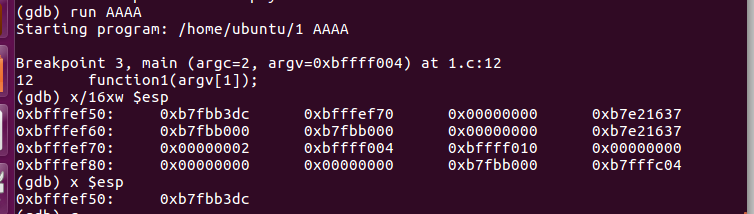
打开文件1



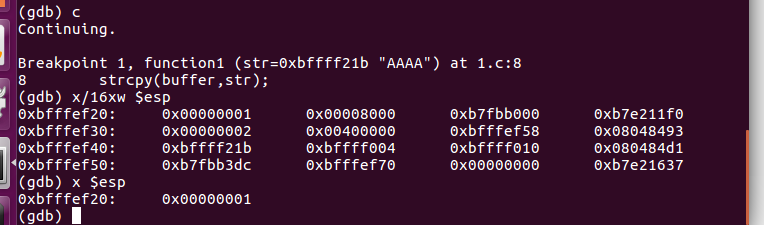
在8，9 12下断点



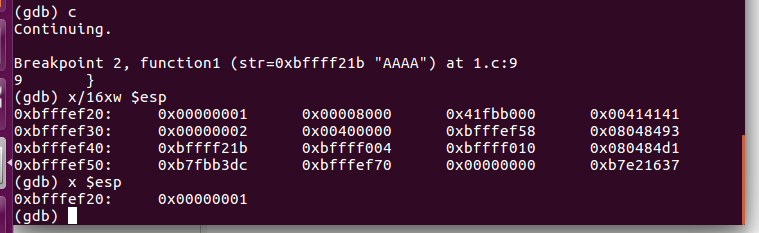
看main处时栈空间的地址内容



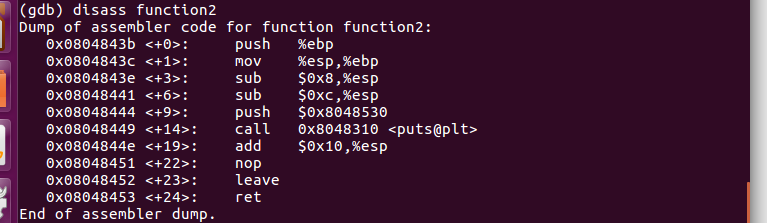
继续运行，看function1处时栈空间的地址内容



继续运行，看function2处时栈空间的地址内容



查看function2的起始地址



精准覆盖返回地址

