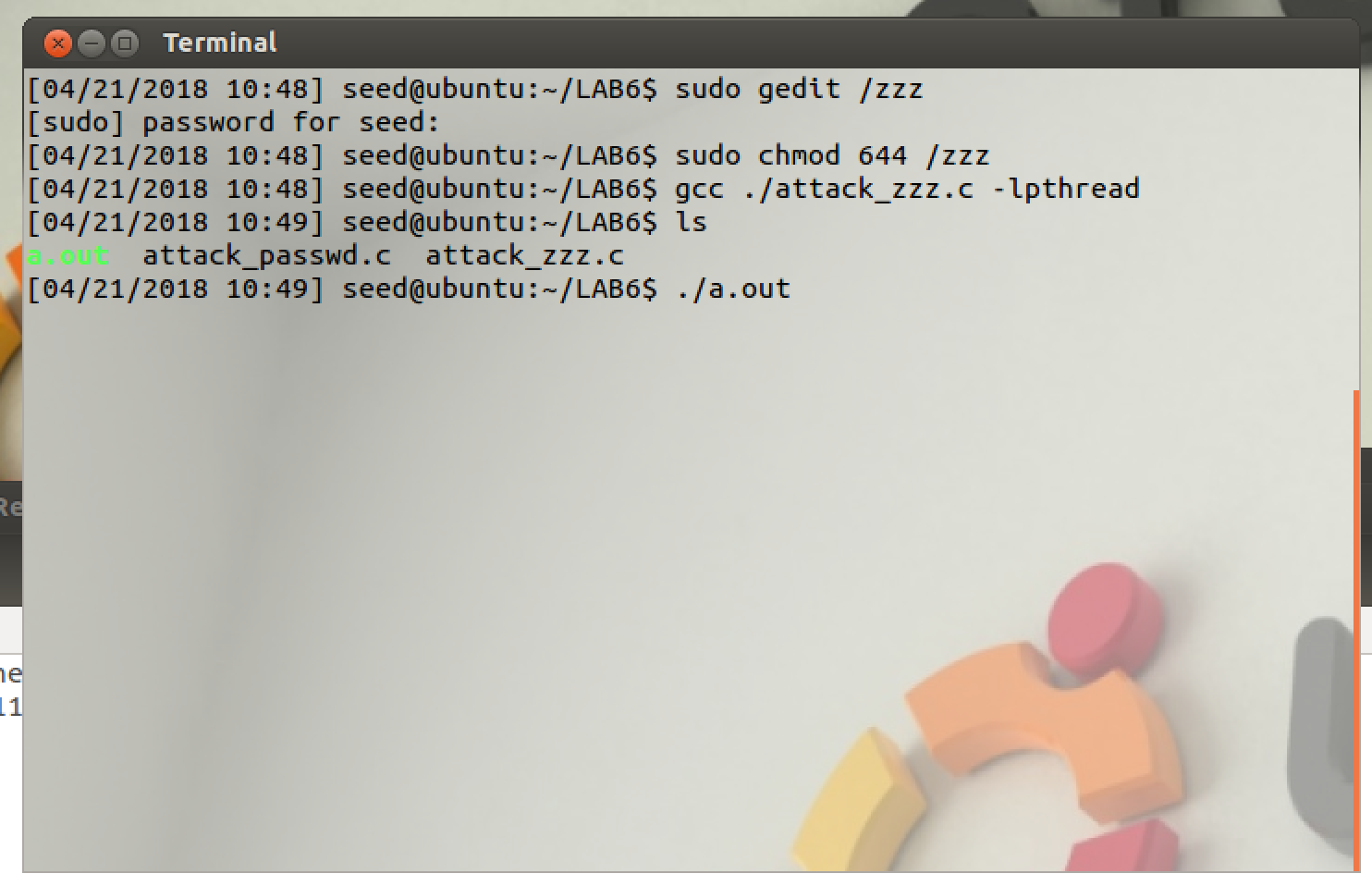
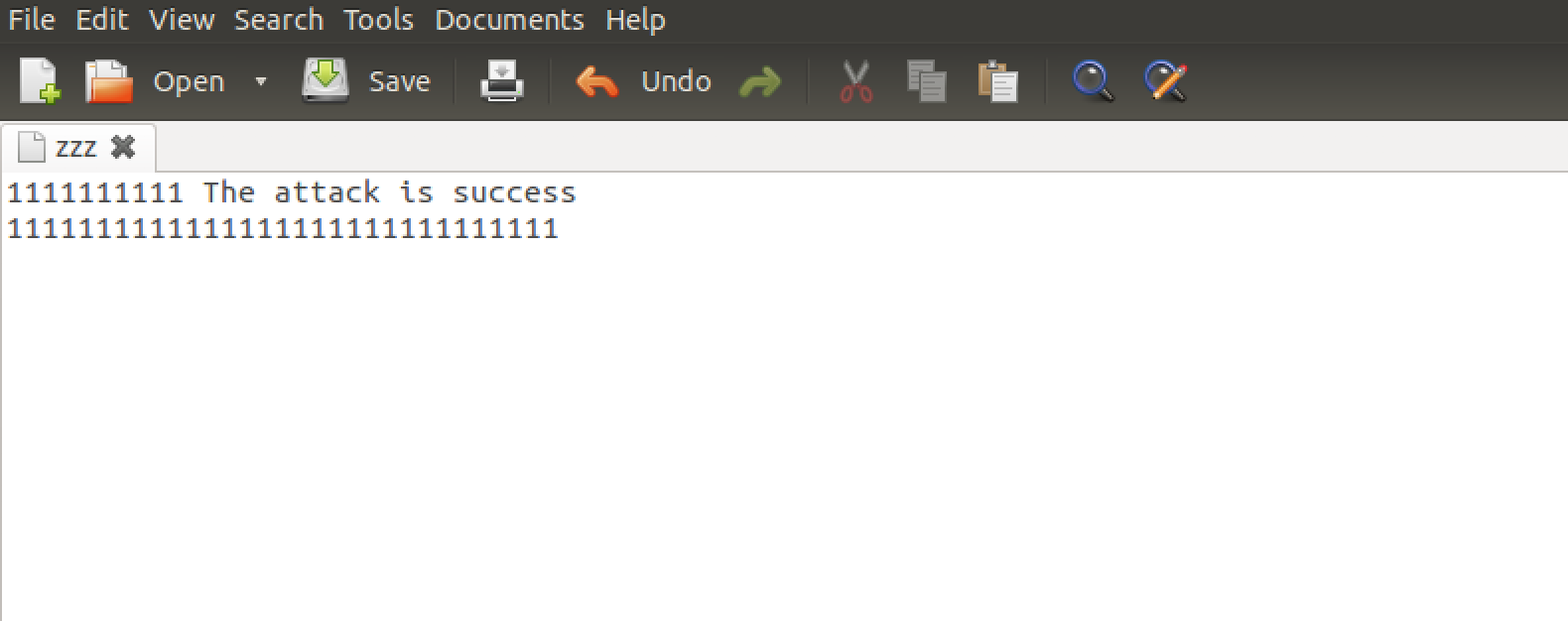
Lab6: Dirty COW Attack Lab

**Task 1: Modify a Dummy Read-Only File**



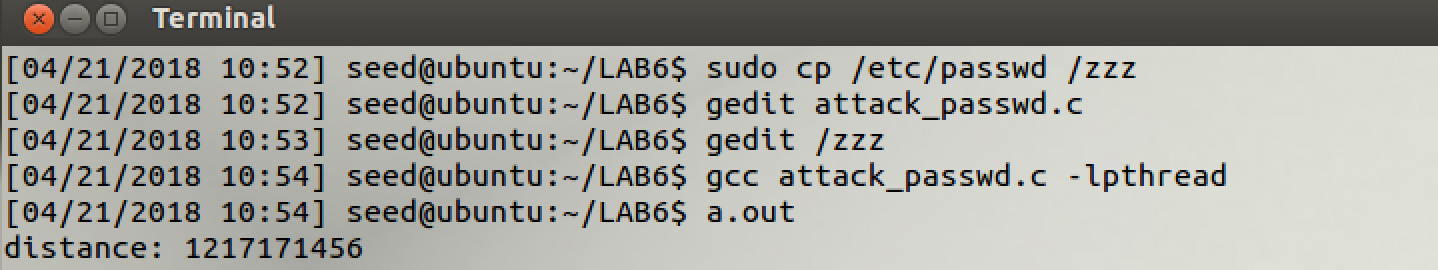
Observation: In this task, I have to modify the file /zzz by exploiting the dirty cow vulnerability. File /zzz has 32 characters of 1. I run our attack\_zzz.c program.

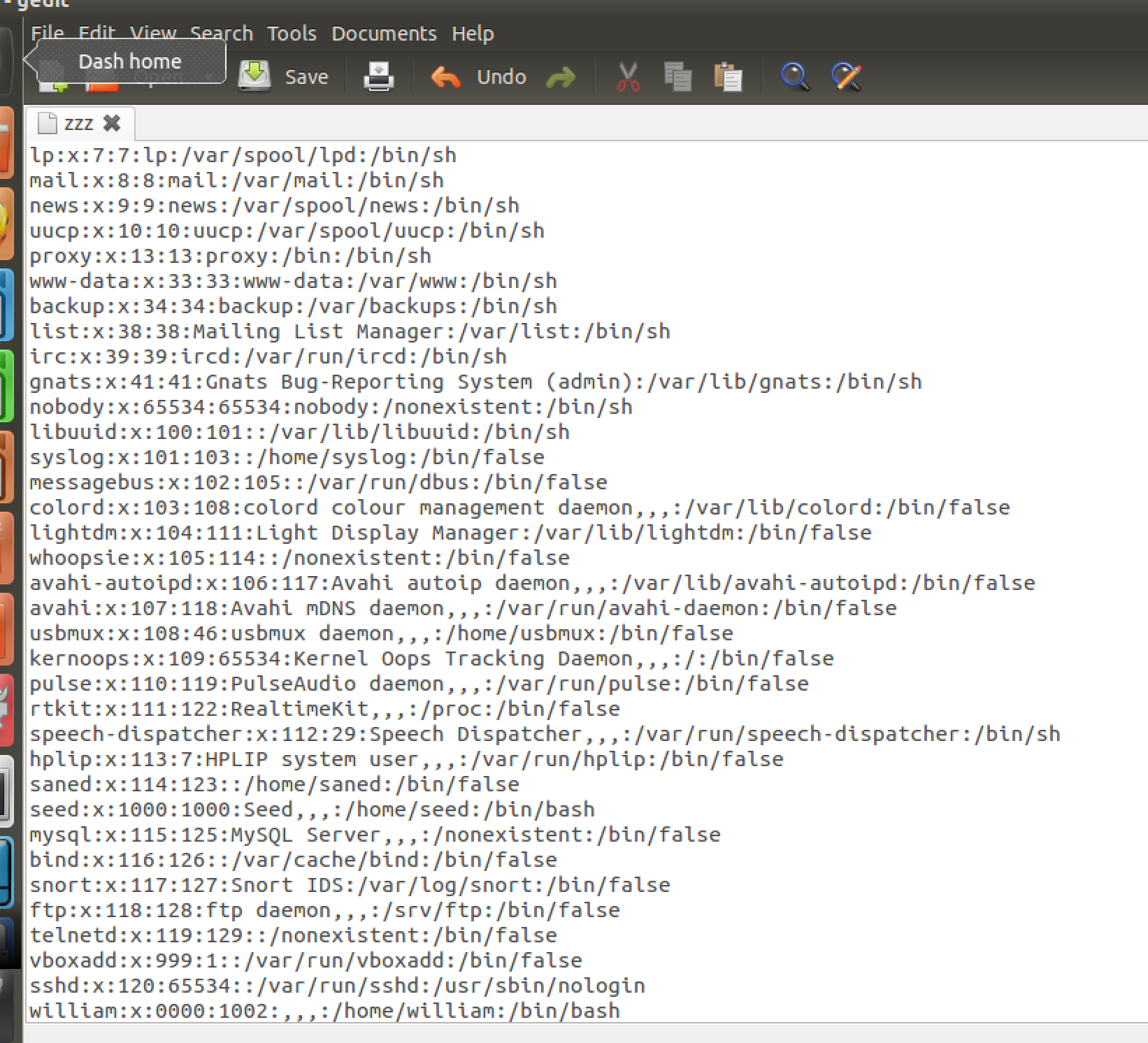


Observation: I can observe that the string has been appended.

Explanation: Ditry COW exploits a race condition in Linux Kernel. There is a race condition on the logic of copy-on write which enables attackers to write to the memory that actually maps to read-only file.

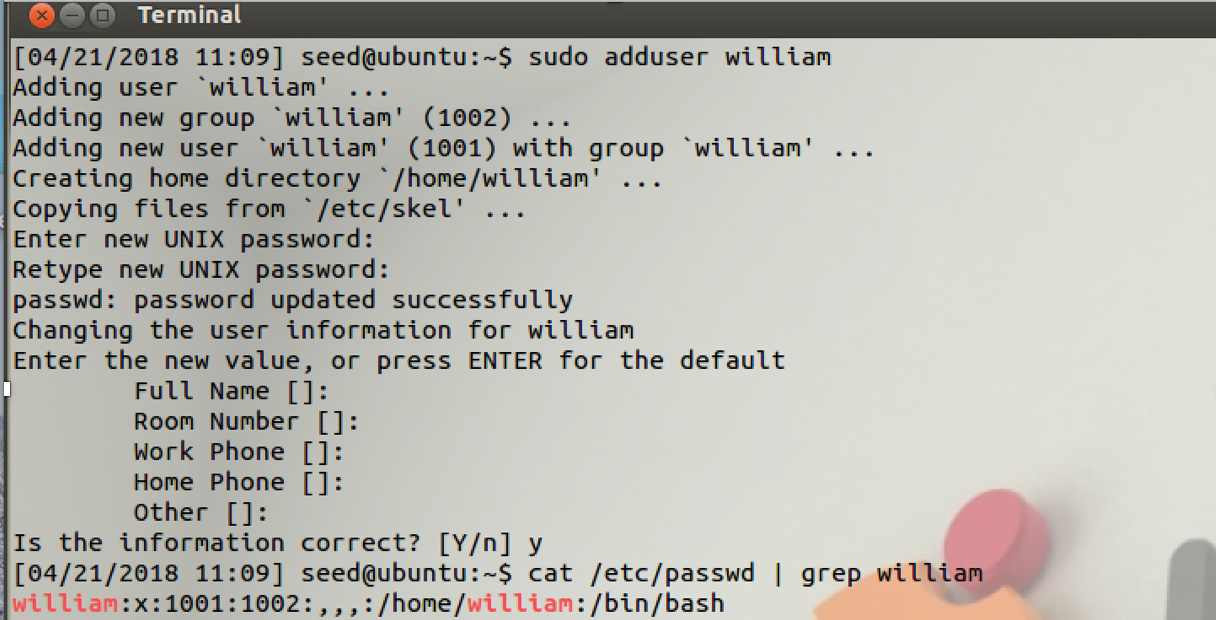
**Task 2: Modify the Password File to Gain the Root Privilege**

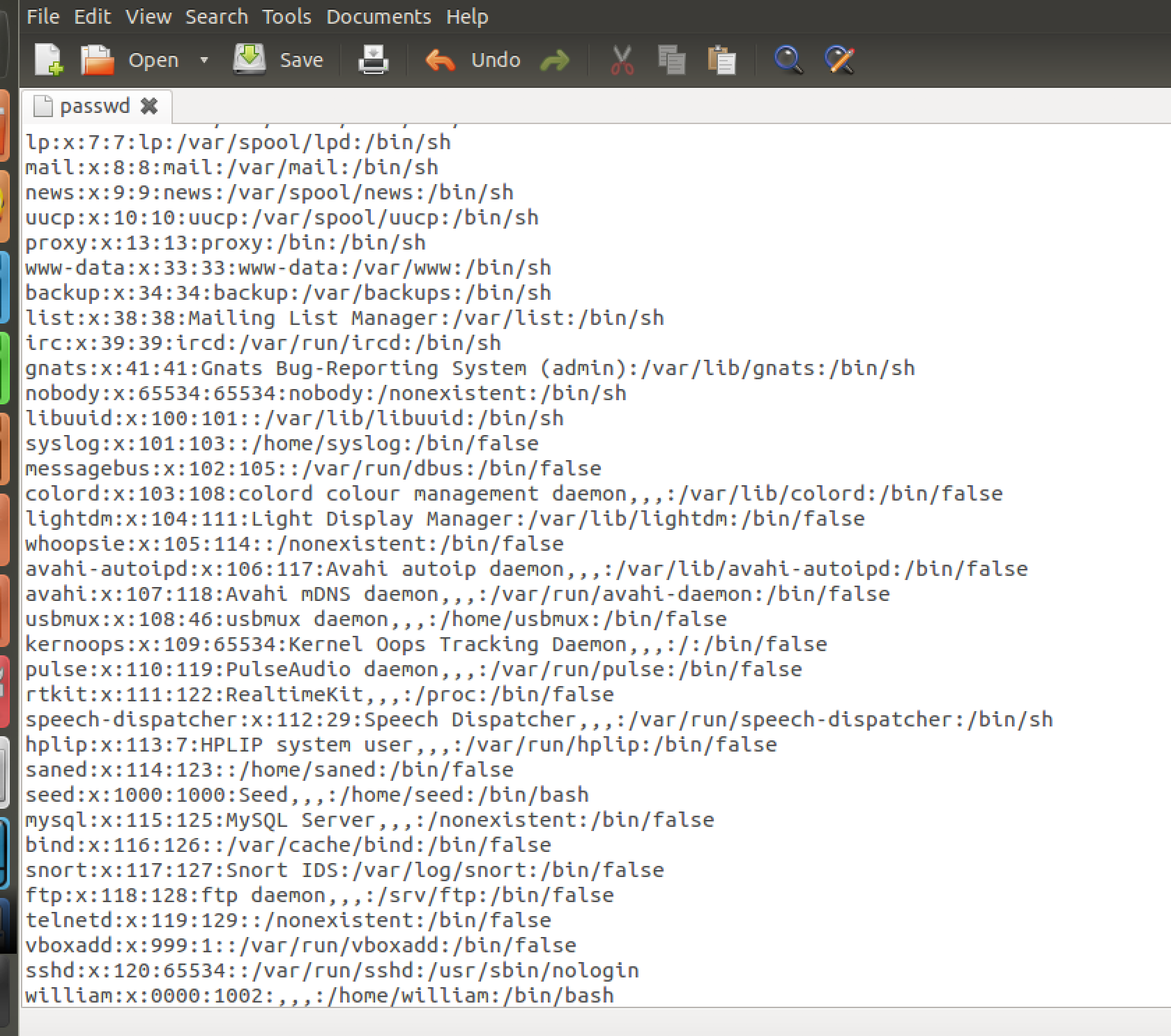
****

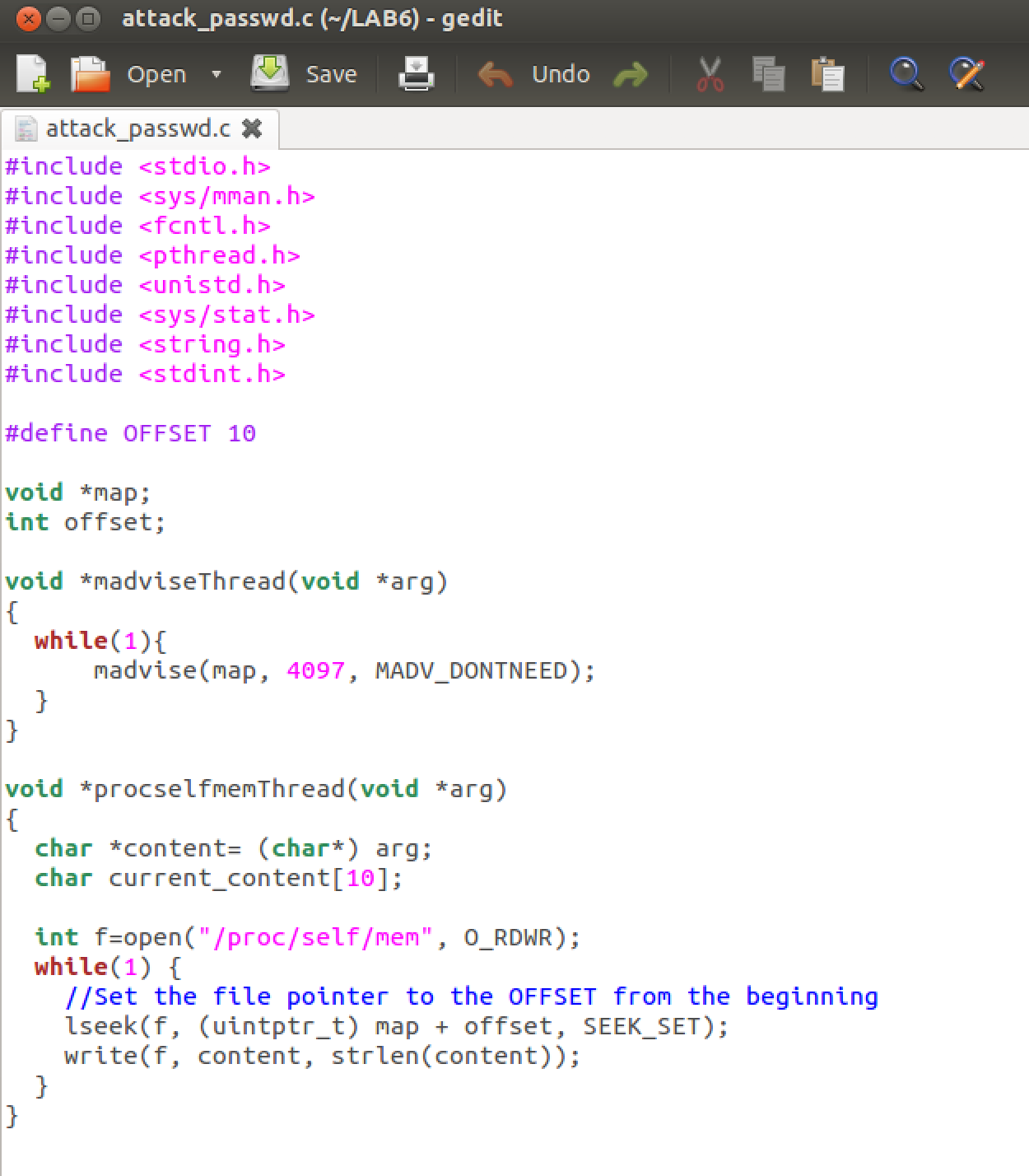
****

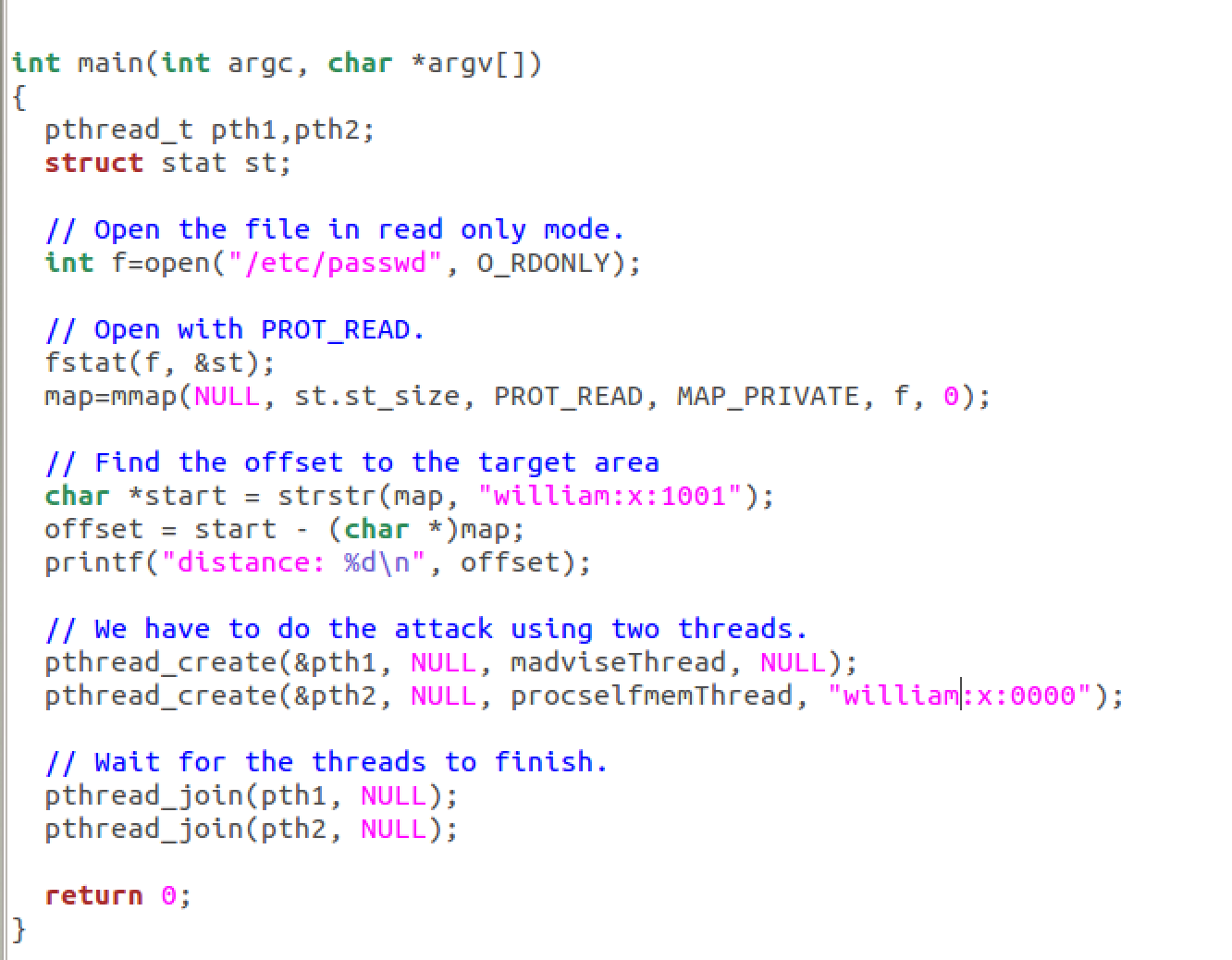
Observation and Explanation: In this task, I copy contents of passwd file into /zzz and attack. I observe that william user has been given root privileges.

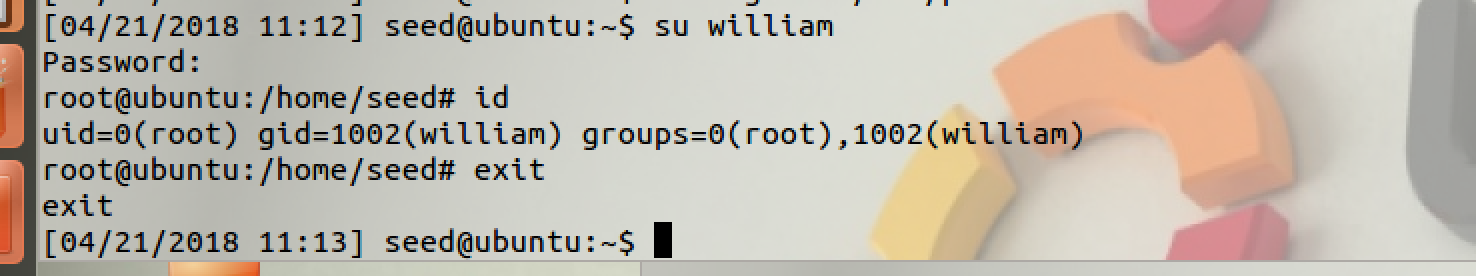
Now I will use this vulnerability to attack /etc/passwd file.











Observation: I use our attacker\_passwd.c program to perform the attack on passwd file and I am successful in giving root privileges to william user.

Explanation: I have successfully exploited the Dirty COW vulnerability to make changes to my /etc/passwd file. Race condition of copy-on-write gets exploited and I get the root access.