# Sudo提权复现报告（CVE-2019-14287）

**朱凯 4042017046**

一、实验要求

1. 掌握sudo提权漏洞原理。
2. 实现具体复现。

二、实验环境

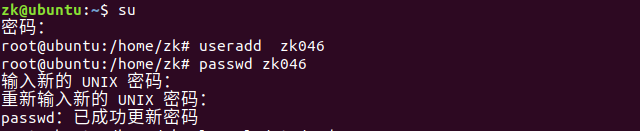
Vm虚拟机，Linux系统（sudo版本<1.8.28）

三、漏洞原理

用户 ID 转换为用户名的函数 会将 -1（或无效等效的 4294967295）误认 为是 0，而这正好是 root 用户 User ID 。此外，由于通过 -u 选项指定的 User ID 在密码数 据库中不存在，因此不会运行任何 PAM 会话模块。

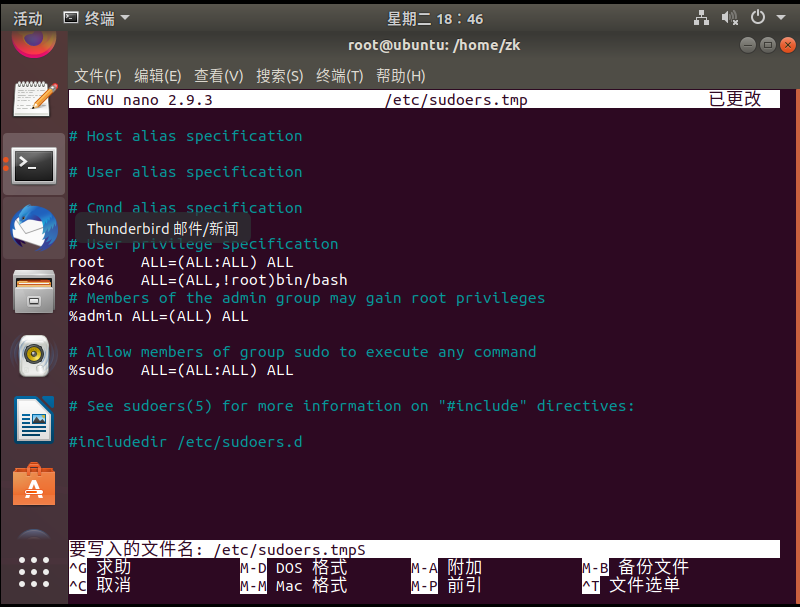
1. 复现过程

添加用户名zk046 并设置密码

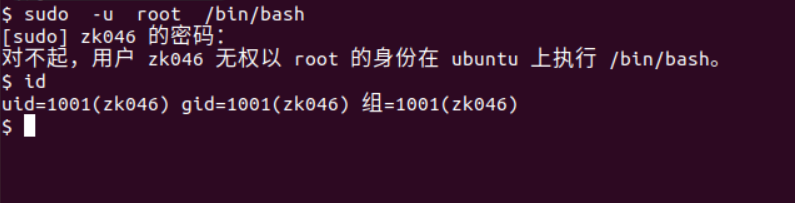


③配置 sudoers 文件

将创建的新用户加入 sudoers 中



1. 正常情况时



1. 运行sudo -u#-1 /bin/bush成功时



1. 实验总结

在该实验中掌握了sudo提权漏洞的原理， 并了解了一些命令行的使用，而且知道了“纸上得来终觉浅，绝知此事要躬行”