Cve-2019-14287 **Sudo提权漏洞分析**

1. 背景知识

2019年10月14日， sudo 官方在发布了 CVE-2019-14287 的漏洞预警。它是由苹果信息安全部门的研究员 Joe Vennix 发现并分析的 。

Linux是多用户多任务的操作系统, 共享该系统的用户往往不只一个。出于安全性考虑, 有必要通过useradd创建一些非root用户, 只让它们拥有不完全的权限; 如有必要再来提升权限执行。

sudo就是来解决这个需求的: 这些非root用户不需要知道root的密码，就可以提权到root，执行一些root才能执行的命令。

执行命sudo -u <用户名> <令>, 将允许当前用户，提权到<用户名>的身份，再执行后面的<命令>, 即使<命令>原本需要root权限。提权到<用户名>身份时，是以<用户名>的身份来执行命令的，因此创建的文件默认属于<用户名>用户。

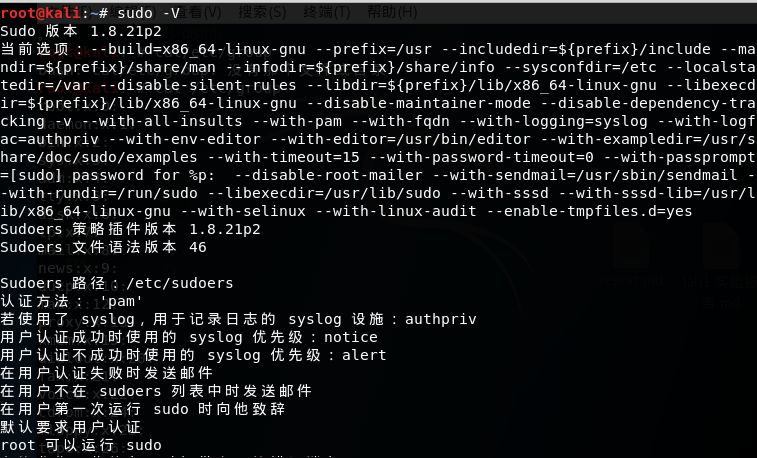
1. 漏洞复现

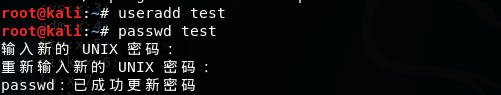
1.查看sudo版本，并创建test用户

I sudo -V 查看sudo版本

II useradd test 添加test用户

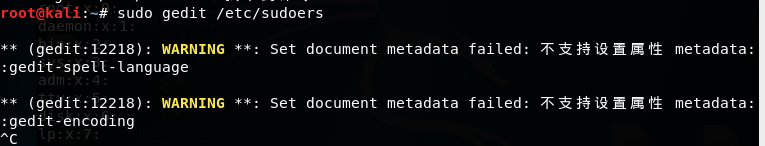
III passwd test 为test用户设置密码

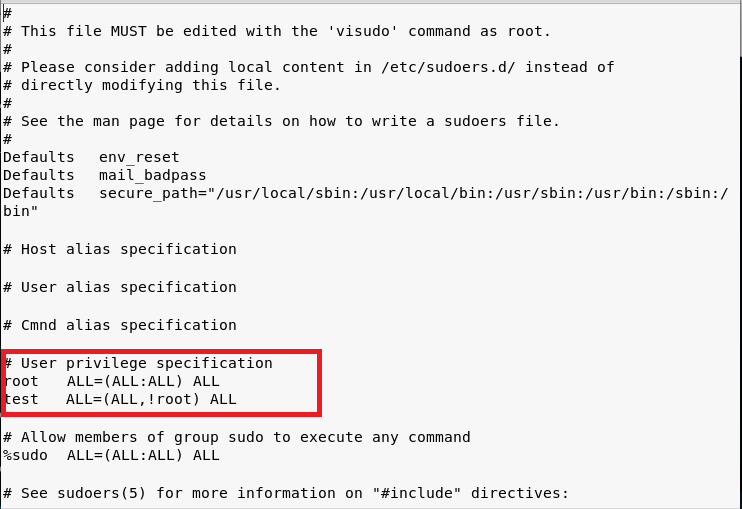




2.修改sudo配置文件：在root ALL=(ALL:ALL) ALL下面添加一行配置test ALL=(ALL,!root) ALL

sudo gedit /etc/sudoers 使用文本编辑器打开sudo配置文件





I test ALL=(ALL,!root) ALL

II test 表示test用户

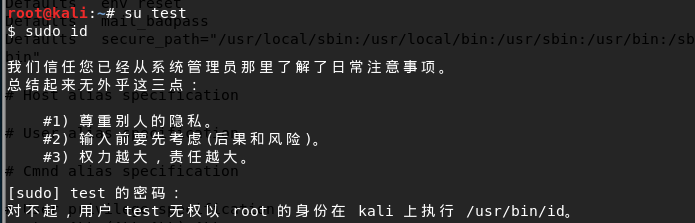
III 第一个ALL表示该用户可以在任意地方使用sudo

IV 第二个(ALL,!root) 表示命令可以被除了root以外的任意用户执行

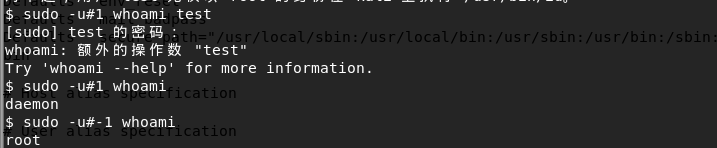
V 最后一个ALL 表示被允许执行

整体表示：test用户可以使用sudo，以除了root以外的任意用户去执行命令

sudo id 查看root用户的ID



* 由上图可以看到，使用命令报错
* 解决方法：sudo -u#数字 命令，其中数字是范围：-1~4294967295，命令是系统命令
* 如果要以root身份去执行命令，数字使用-1或4294967295，至此漏洞复现成功！！
  + 命令中的数字是id号，可以在/etc/group中查看



1. 漏洞原因

产生这个漏洞，是因为将用户 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. 限制条件

1.Sudo版本低于1.8.28；

2.知道用户的密码；

3.用户处于sudo权限列表之中。