Sudo提权漏洞分析与复现

**漏洞背景**

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 。

**关于sudo**

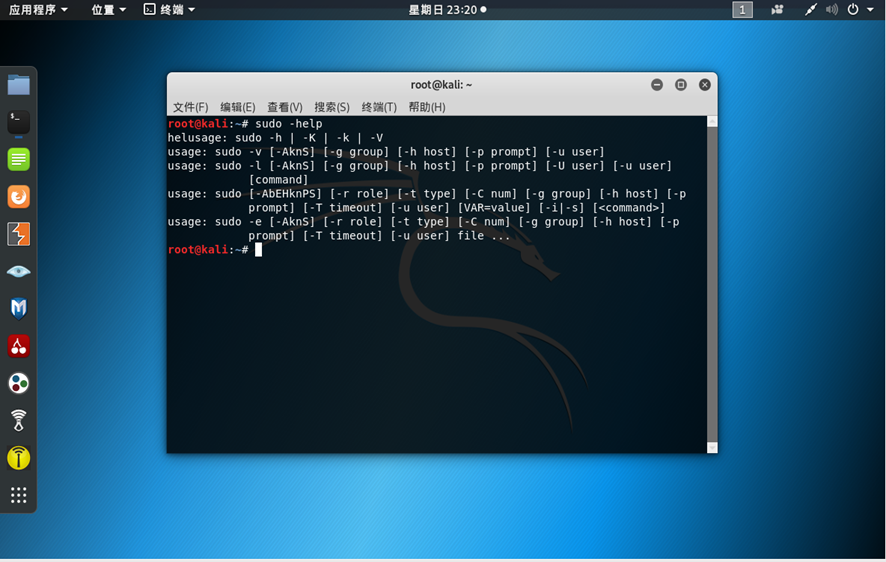
Linux是多用户多任务的操作系统, 共享该系统的用户往往不只一个。出于安全性考虑, 有必要通过useradd创建一些非root用户, 只让它们拥有不完全的权限; 如有必要再来提升权限执行。

　　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。

如果不带-u, 则默认使用root用户，而大多数时候sudo都是要提权到root的，所以-u <用户名>可以省略为:

sudo <命令>

需要注意的是: 执行sudo时输入的密码是当前用户的密码, 并非<用户名>的密码。



**/etc/sudoers内容**

sudo的权限控制可以在/etc/sudoers文件中查看到。一般来说，通过cat /etc/sudoers指令来查看该文件, 会看到如下几行代码:

root ALL=(ALL:ALL) ALL

%wheel ALL=(ALL) ALL

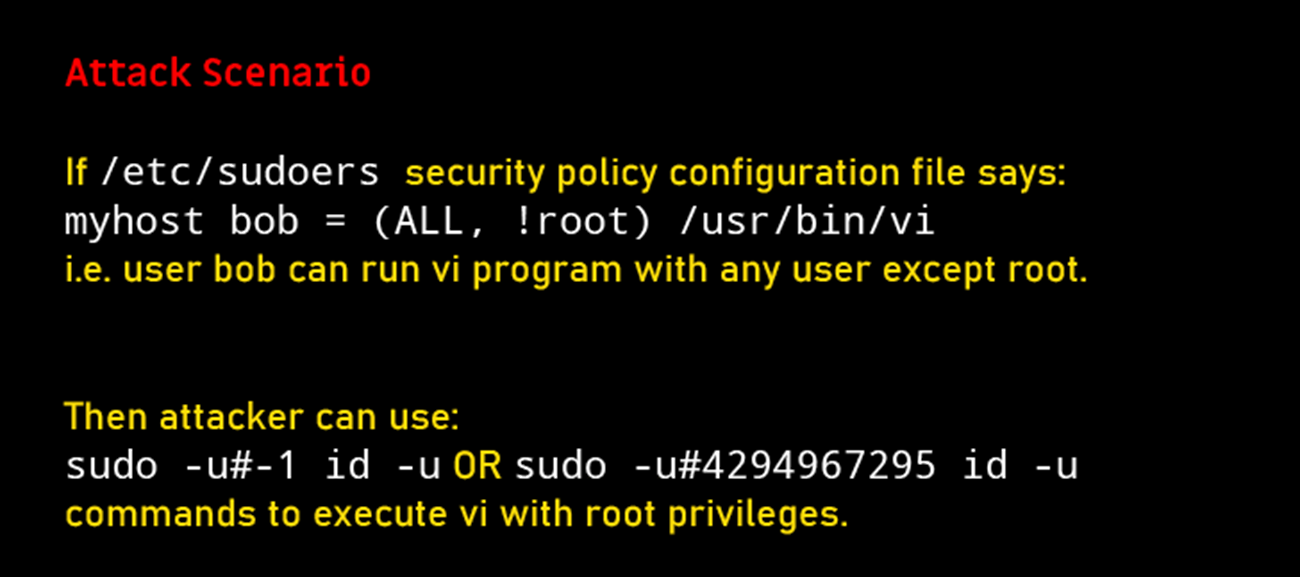
%sudo ALL=(ALL:ALL) ALL

　　对/etc/sudoers文件进行编辑的代码公式可以概括为:

授权用户/组 主机=[(切换到哪些用户或组)] [是否需要输入密码验证] 命令1,命令2,...

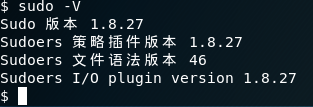
（详解：https://my.oschina.net/aiguozhe/blog/38706）

**漏洞复现**



**信息查看**

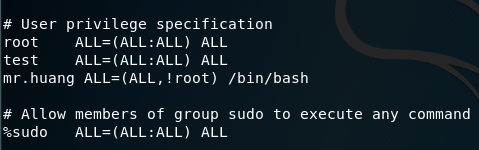
查看sudo版本



查看 /etc/sudoers内容



找到ALL关键字行，查看是否有可以利用该漏洞的定义语句（一般情况下没有这种语句，需要自己写到/etc/sudoers文件中 具体操作这里不做介绍）

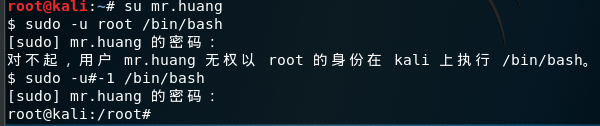


看到 mr.huang ALL=(ALL,!root) /bin/bash ，可以利用漏洞

**漏洞利用**

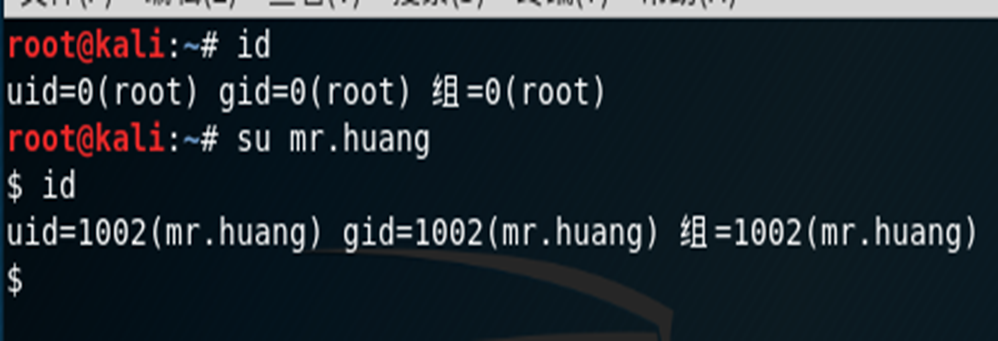
先切换到用户mr.huang 命令：su mr.huang

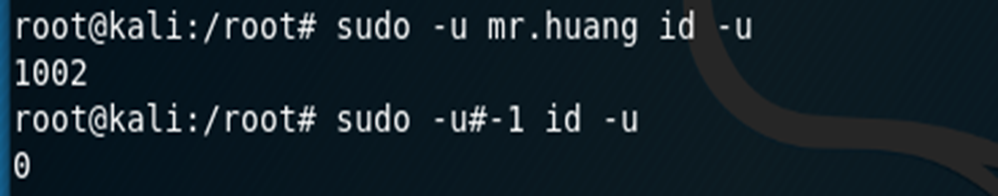
mr.huang ALL=(ALL,!root) /bin/bash 这句话表示禁止mr.huang以root身份执行/bin/bash命令，进行尝试会被拒绝，“对不起，用户 mr.huang 无权以 root 的身份在 kali 上执行 /bin/bash。”接着利用漏洞尝试，命令：sudo -u#-1 /bin/bash,尝试发现会直接从mr.huang切换到root，提权成功



**漏洞分析**

之所以会产生这个漏洞，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。





**条件限制**

Sudo版本低于1.8.28

知道用户的密码

用户处于sudo权限列表之中

存在 ALL 关键词的复合限制逻辑

**漏洞影响**

CVE-2019-14287漏洞影响1.8.28之前的Sudo版本。尽管该错误功能强大，但重要的是要记住，只有通过sudoers配置文件为用户提供了对命令的访问权限，它才能起作用。如果不是这样，并且大多数Linux发行版默认情况下都没有，那么此错误将无效。大多数Linux服务不受影响。360cert将其定为低危漏洞