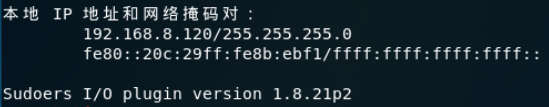
Sudo提权漏洞复现过程

1、 查看sudo版本

Sudo –V

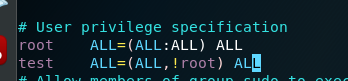


只要是小于1.8.28版本的sudo都会出现这个漏洞

2、 修改配置文件

gedit /etc/sudoers打开sudoers文件，在root(ALL:ALL)ALL行下面添加一行

test ALL=(ALL,!root)ALL



第一个ALL表示用户可以在任意地方使用sudo

第二个（ALL,!root）表示命令可以被除了root以外的任意用户执行

最后一个ALL表示允许被执行

整体代码：test用户可以使用sudo，是除了root以外的任意用户去执行

3、创建test用户并切换：

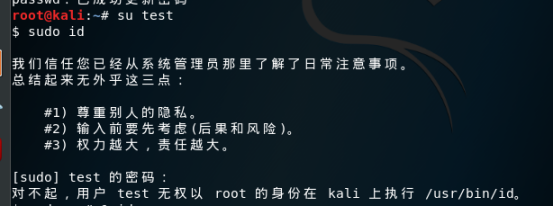
useradd  test

passwd test



Su test切换至test用户

然后sudo id（查看root的ID）



发现没有权限执行

4、 使用以下方法去执行想要的执行的命令



Sudo –u#数字 命令

其中数字范围：-1~4294967295，命令是系统命令

数字-1或者最大代表root用户

因为命令在将UID转换为对应用户时，会将-1或4294967295这两个异常数字视为0，而0是root用户的UID,这样就相当于获得了root用户的权限。

总结：虽然sudo提权看起来使普通用户获得root权限，但是它只能在某个用户通过sudoers文件的配置访问某个命令的权限时才能生效。如果不是这种设置——大多数Linux发行版默认都不是——那么这个漏洞将不会产生任何影响。也就是说这个漏洞只能在非标准配置的Linux下生效，大多数Linux服务器不受影响，所以这个漏洞的局限性非常大。