### sudo提权漏洞实验报告

**相关知识：**

sudo是linux的系统命令，当在Linux操作系统上执行命令时，只有得到许可或者知道root密码，普通用户才可以使用sudo（super user do）命令以root身份执行命令。因此对于sudo命令来说，通过向/etc/sudoers配置文件添加特殊的指令，就可以让某个用户以另一个用户的身份运行命令。但是该漏洞可以使普通用户绕过相关安全策略、获取root权限，从而执行敏感命令。

**漏洞原因：**

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，从而获取到root权限。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，从而对用户透明。

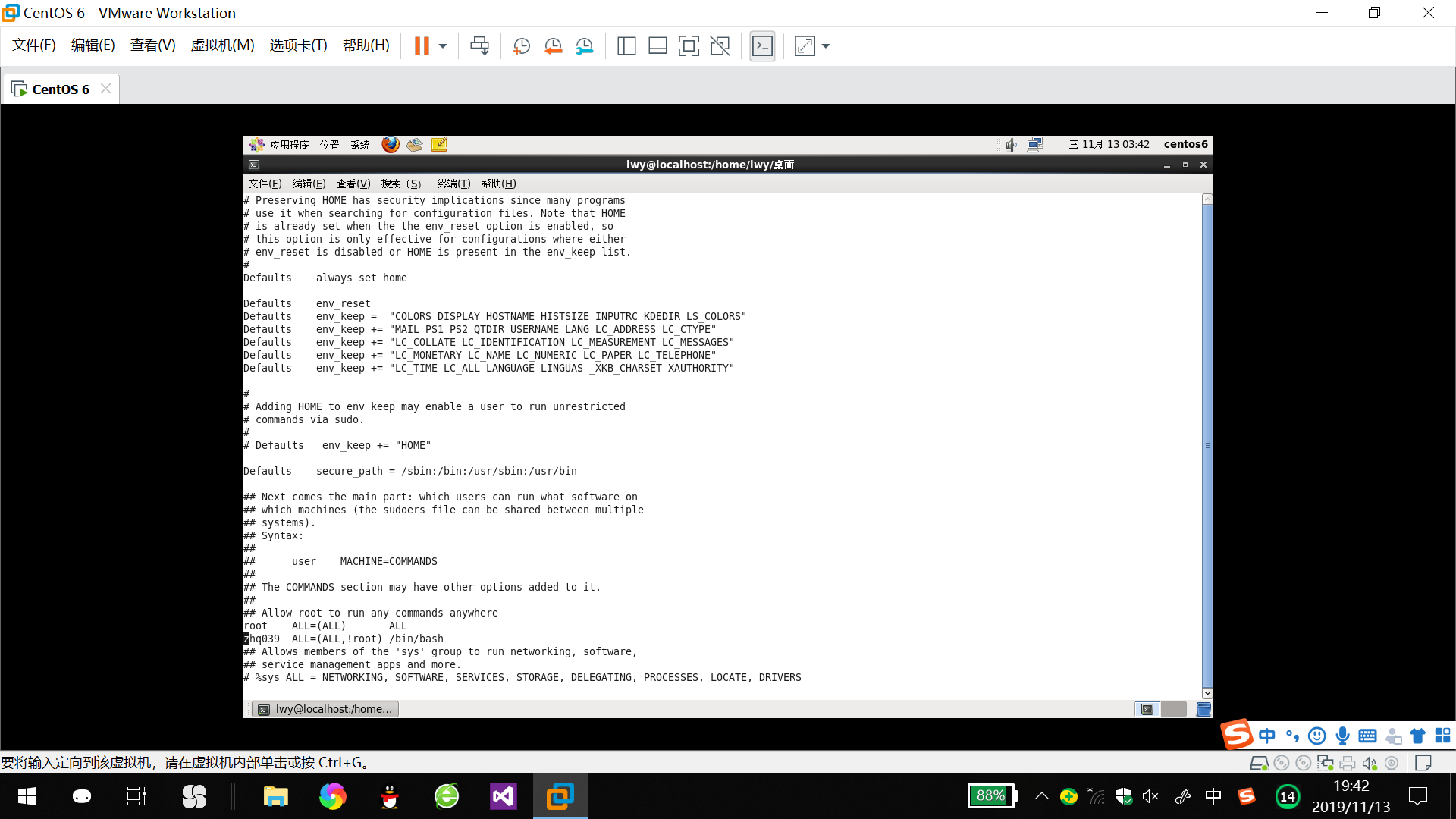
**复现漏洞：**

1. 查看sudo的版本，因为新版本已经对该漏洞进行了修复。 1.8.28之前的sudo版本均会受到影响。

可以通过Sudo –V命令进行查询。

QQ图片20191113203946

1. 修改配置文件，创建新的用户

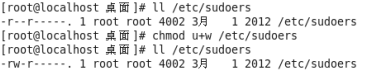


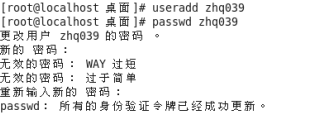
第一个ALL表示用户可以在任意地方使用sudo;

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：zhq039用户可以使用sudo，是除了root以外的任意用 户去执行。

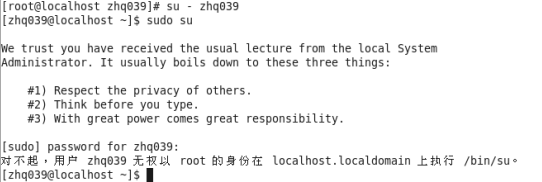




SW115DYR`U3`BT@E1(YE~E5

以root权限 加入用户到sudoers文件中

3、正常步骤执行命令访问



4、漏洞访问

执行 sudo -u#-1 /bin/bash 后直接切换到root权限

D5J$KTOKRWRD0PS1RF[J3KD

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。

**漏洞缺陷:**

1.知道当前普通用户的密码。

1. 当前普通用户在souduers文件中。
2. 本地提权需要本地操作 估计远程ssh连接的终端会失败。

**实验总结：**

经过本次实验，首先是增加了对Linux漏洞的理解，尽管这个漏洞比较简单，但能够真正的复现也体会到了其中的乐趣；其次，对于Linux命令有了更加深入的认识，尤其是在root权限方面。同时在本次实验中也出现了一些问题，比如在创建新用户的时候，没有赋“写”的指令，导致无法将用户导进sudoers文件中去。表明自己对于Linux命令的认识还是很浅薄的，需要进一步加强。