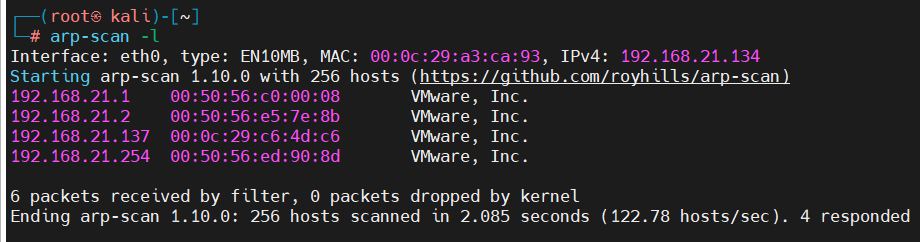
Empire\_LupinOne

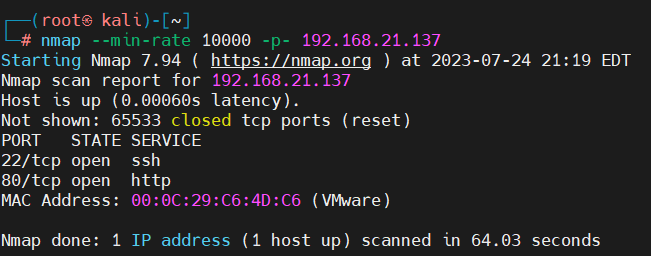
下载地址：忘记在哪下的了，查了一下是vulnhub但是vulnhub没找到

主机发现

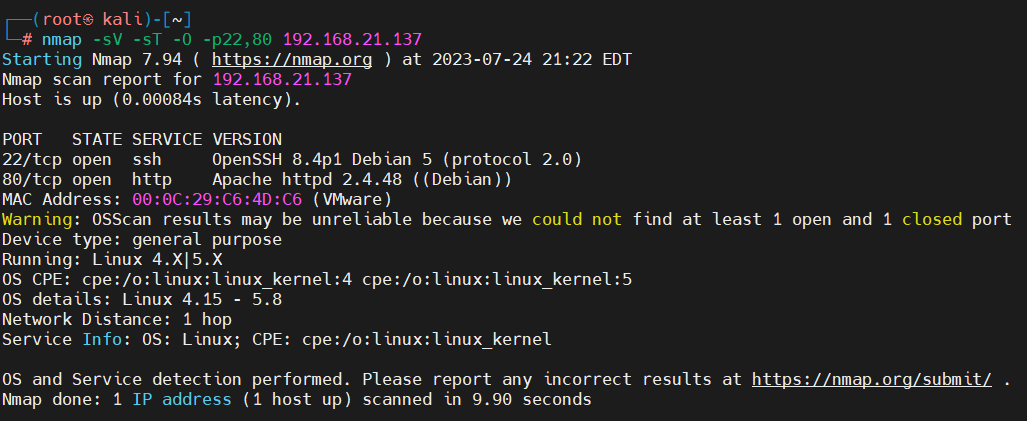
arp-scan -l



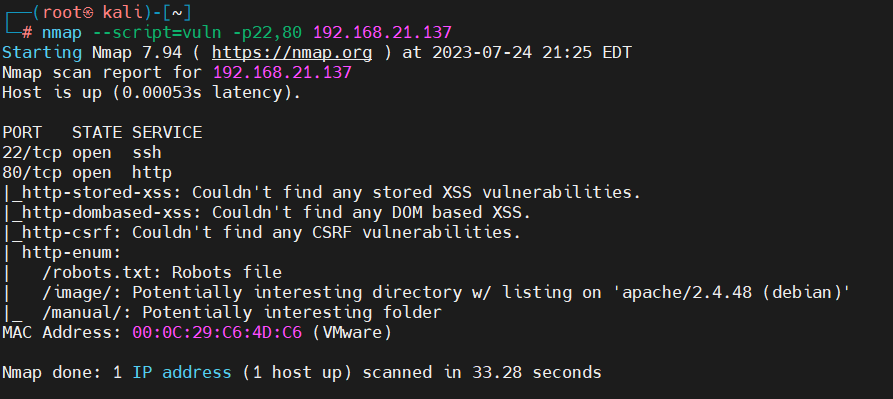
nmap --min-rate 10000 -p- 192.168.21.137



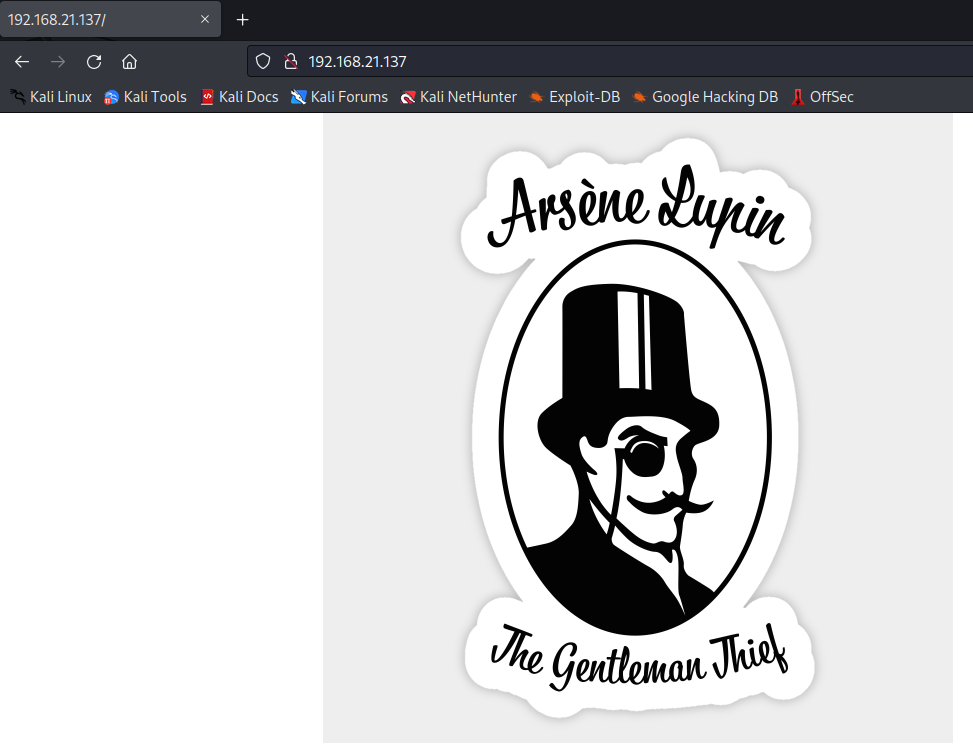
nmap -sV -sT -O -p22,80 192.168.21.137



nmap --script=vuln -p22,80 192.168.21.137

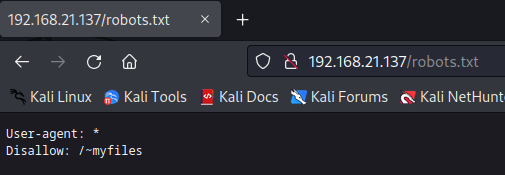


先看一下网页

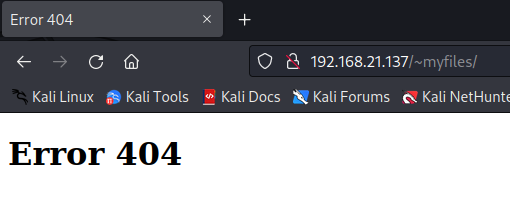


啥也没有

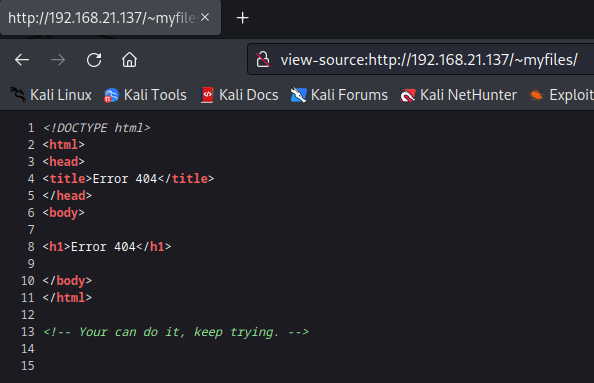
先看一下nmap扫出来的文件



好东西有个~myfiles，先看一下



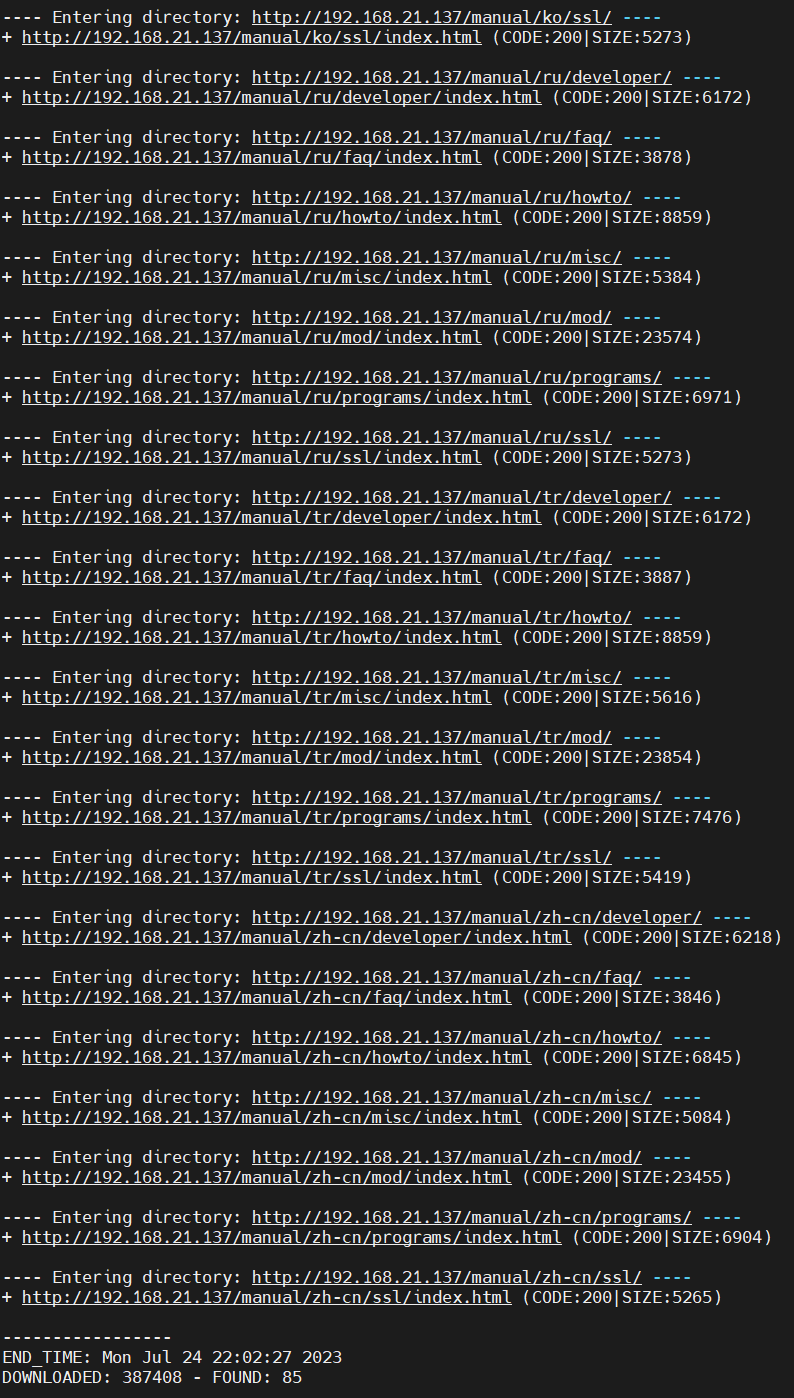
这个要看一下源码了



典型的要我接着爆破文件目录

几个文件试了以后发现dirb好用就用这个吧

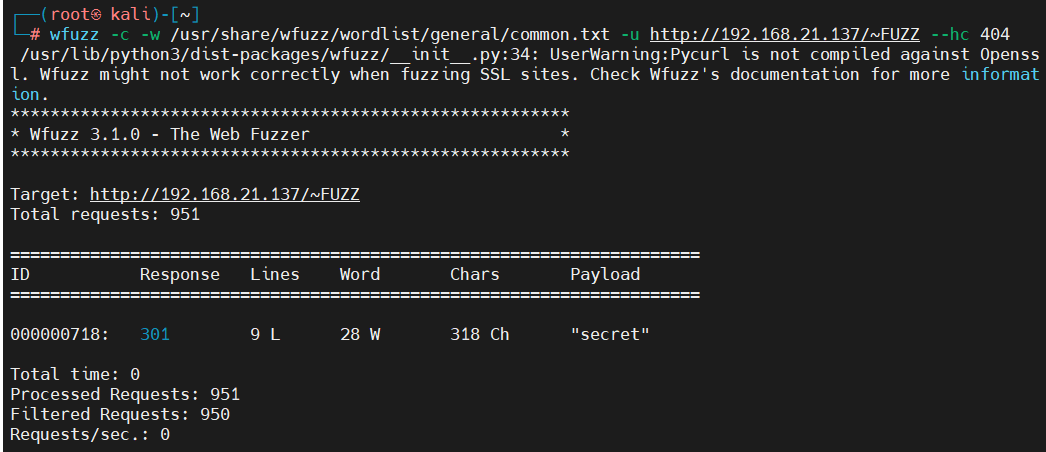
dirb http://192.168.21.137



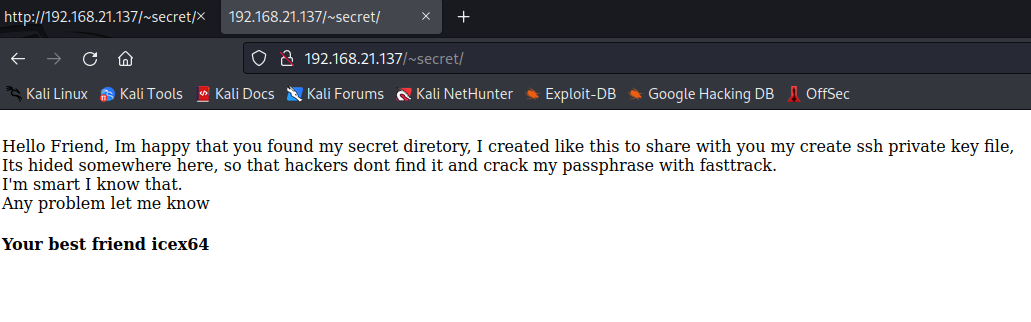
发现这里面有点问题

但是还是找不到有用的文件夹，我就想着是不是和robots提示的文件夹一样前面有~，然后就找到了这个

wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt -u http://192.168.21.137/~FUZZ --hc 404

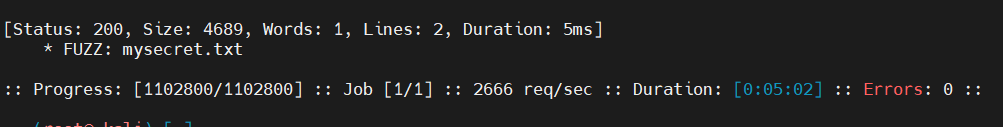


既然搜出来了然后进去看看

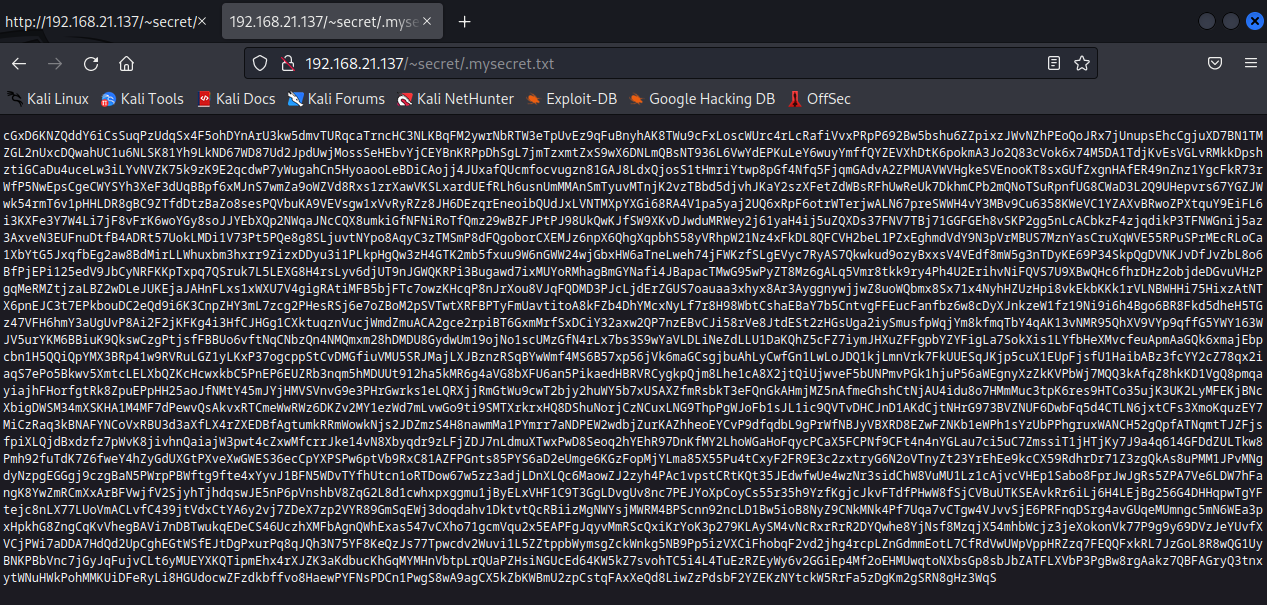


看到了这个告诉了我们要接着扫，这里面还有一个ssh私钥文件，还告诉了我们icex64这里需要我们指定文件的后缀名，就需要使用ffuf了

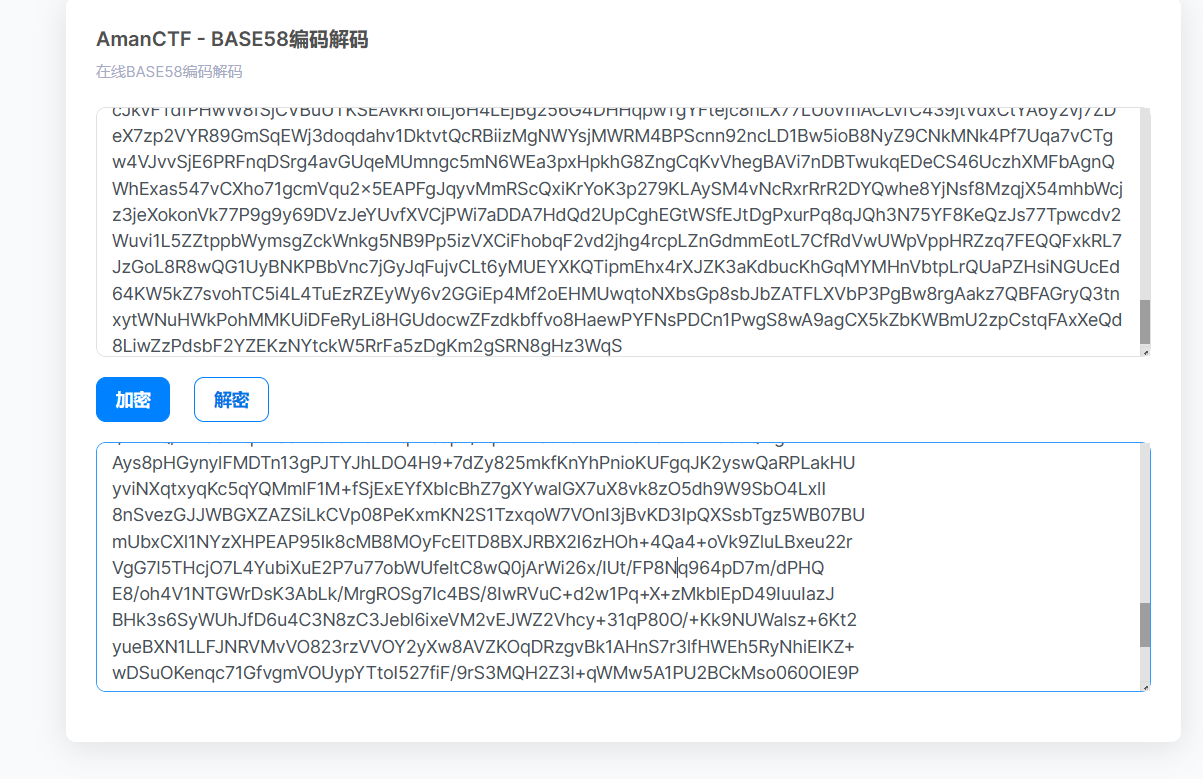
wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt -u http://192.168.21.137/~FUZZ --hc 404



先看一下咯



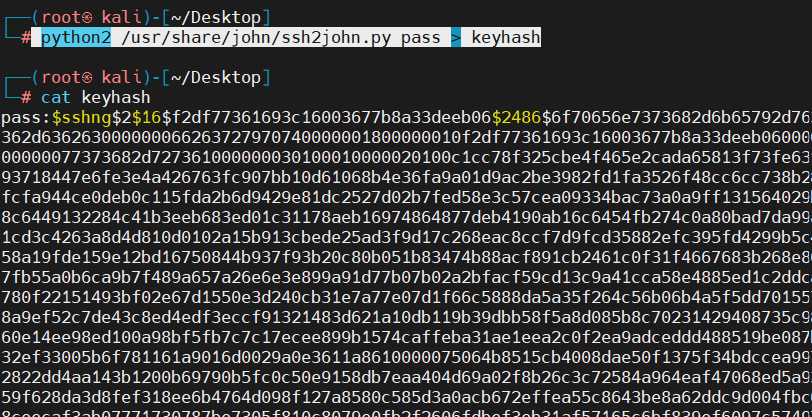
[BASE58编码解码 - Bugku CTF](https://ctf.bugku.com/tool/base58)



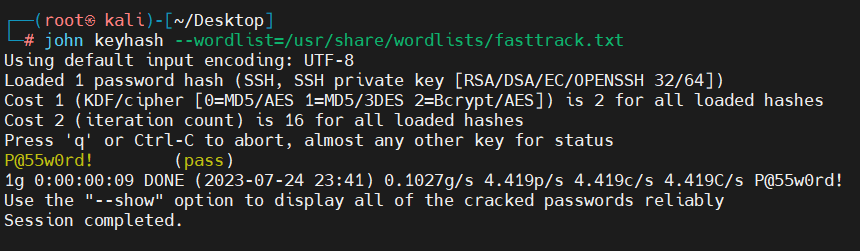
Ok有ssh密钥了保存下来

需要吧ssh2john生成密码再用john爆破

python2 /usr/share/john/ssh2john.py pass > keyhash

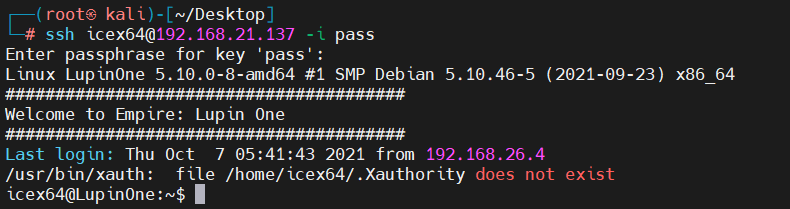


john keyhash --wordlist=/usr/share/wordlists/fasttrack.txt



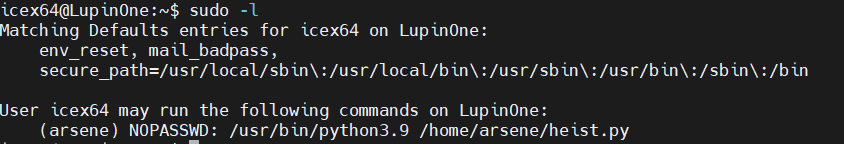
P@55w0rd!

记得要把密钥权限改600



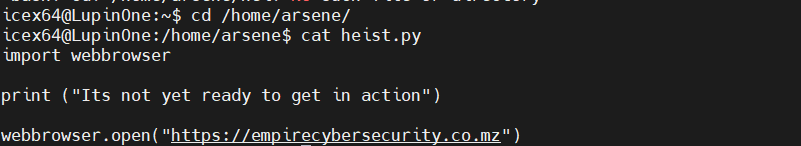
登入成功，接下来看看权限

sudo -l



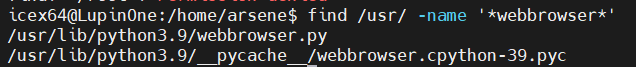
找到heist.py有权限

先去看看

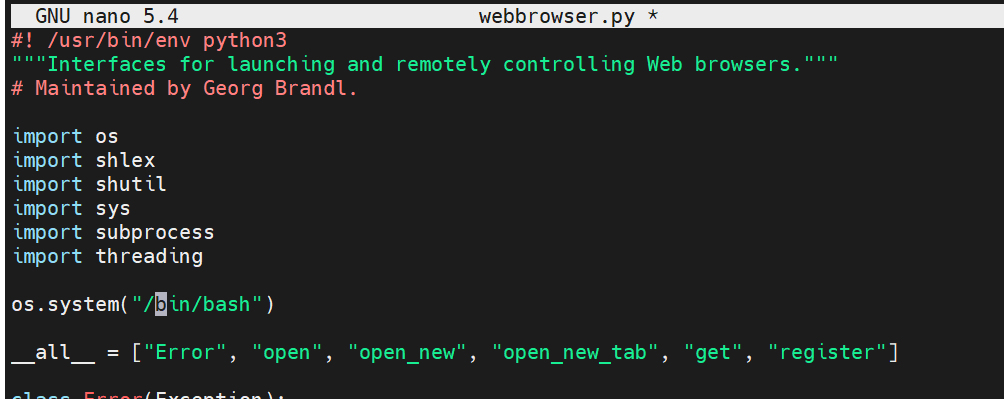


有调用先看调用

find /usr/ -name '\*webbrowser\*'

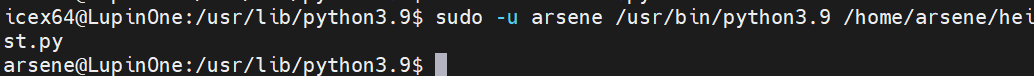


是将此文件打开运行，编辑文件加一个shell脚本

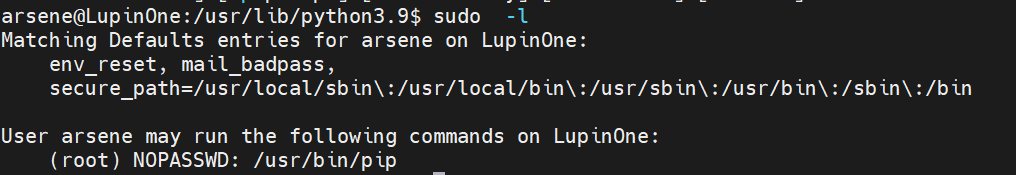


拿到arsene的shell

sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py

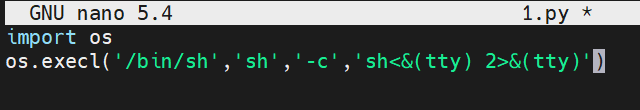


轻松拿到，老样子

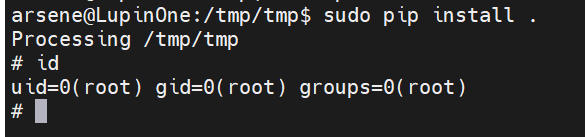


免密执行pip

利用python提权（记得在tmp目录下）



应该用setup做文件名



搞定

