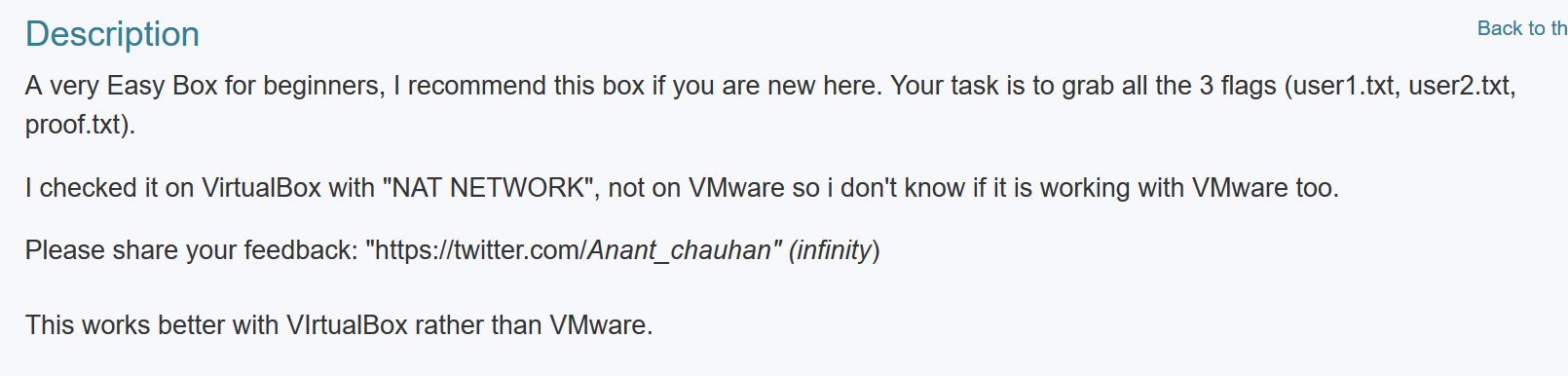
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/tenderfoot-1,581/>

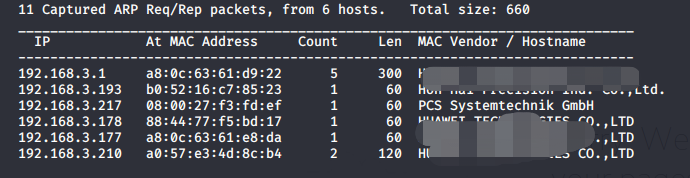
新手级别，3个flag在virtualbox下进行做完以后才发现这是对新手的毒打，由于是virtualbox这里就偷懒了



# 0x01:探测靶机

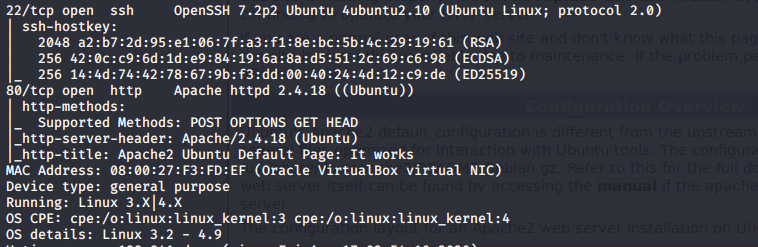
还是先用netdiscover探测一波,直接找PCS可以确定靶机IP为192.168.3.217

命令:netdiscover -r 192.168.3.0/16

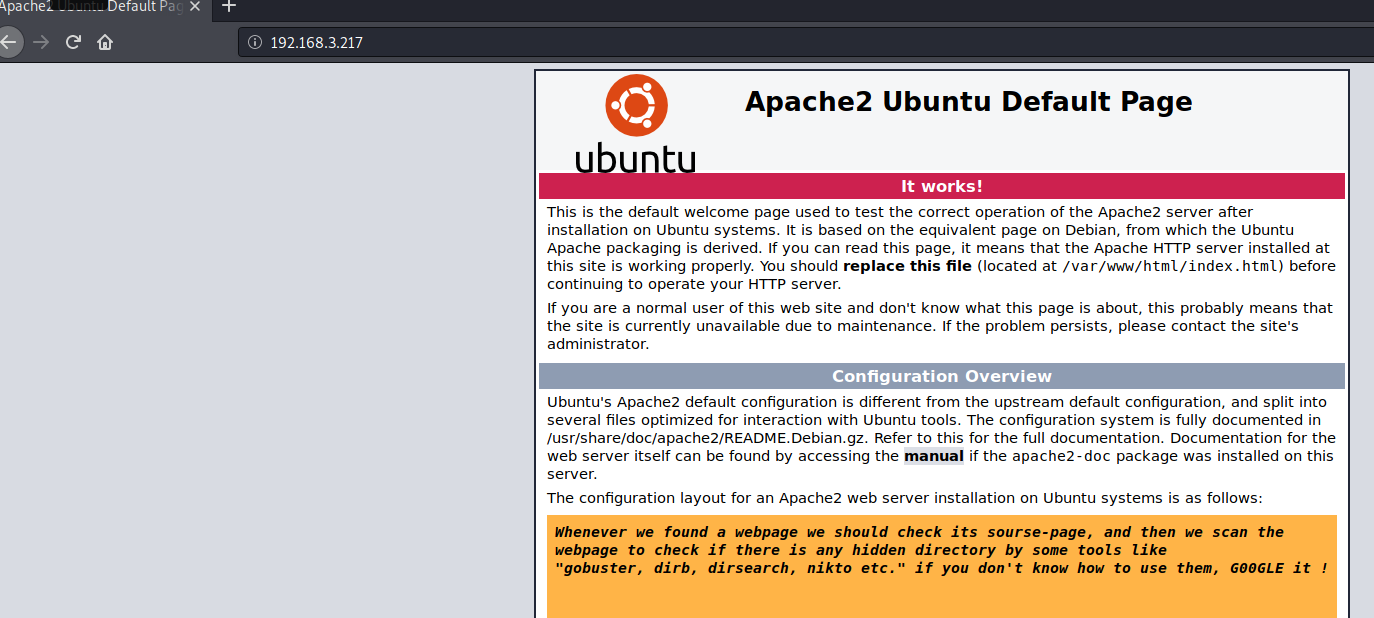


然后开始用nmap扫一波端口，这次只开了22和80端口

命令:nmap -A -sS -sV -v -p- 192.168.3.217

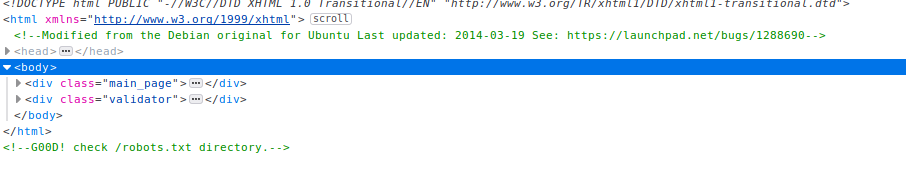


访问一波IP可以正常回显，同时建议我们先查看源代码，再用目录扫描器开挖



# 0x02:挖掘信息

既然说先查看源代码那么先按F12找到点提示，建议我们去查/robots.txt



然后去到/robots.txt的时候在F12，看到一个建议我们去/hint找点东西



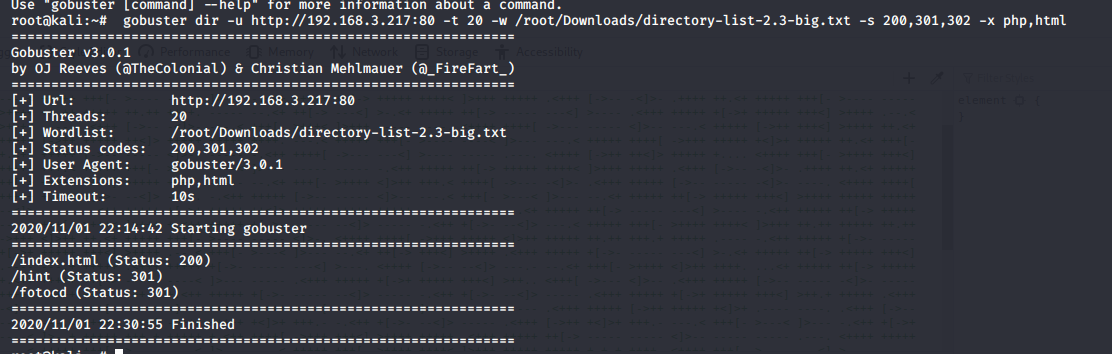
进去以后按住F12有串代码，应该是base64或base32



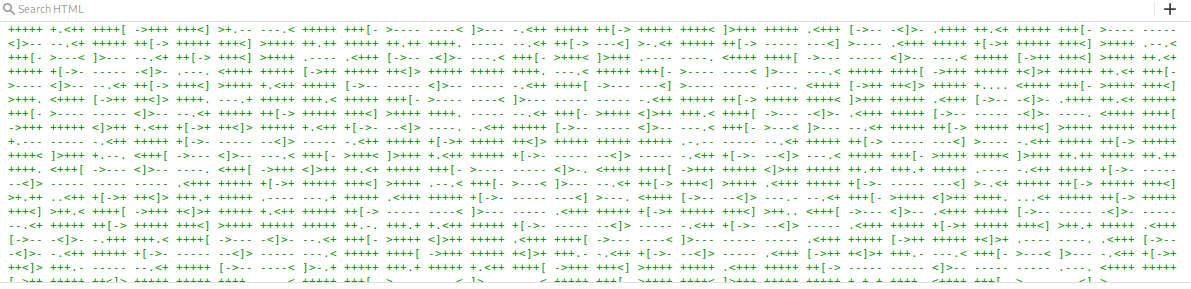
结果。。。。。。。裂开被人调戏了



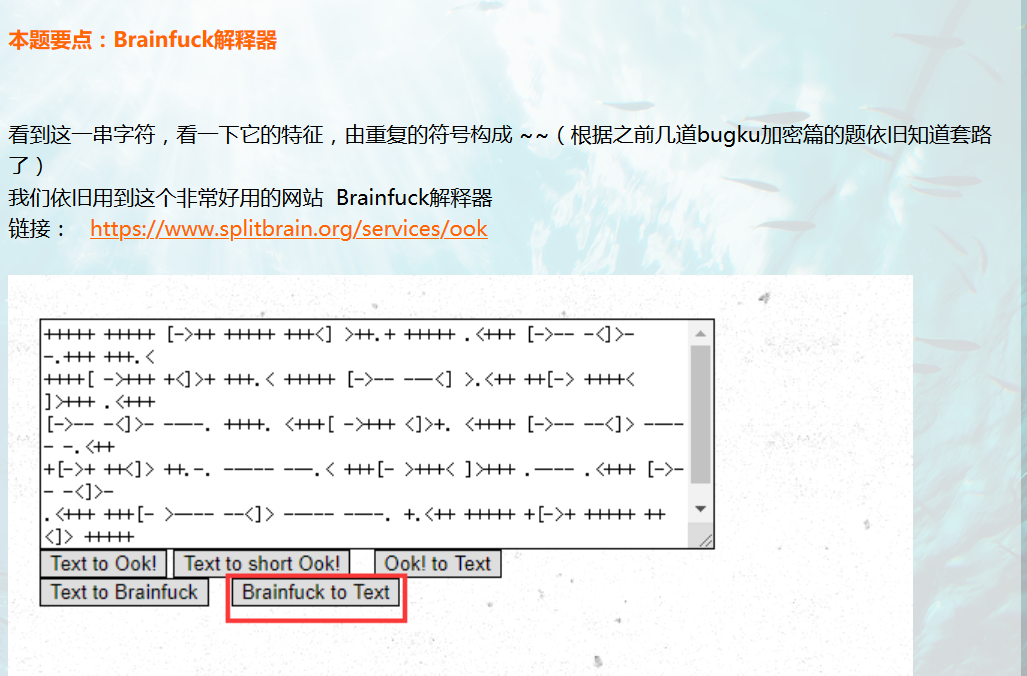
直接上gobuster专门配一个大字典Kali是没有的专门下载了一个，扫到一个/fotocd



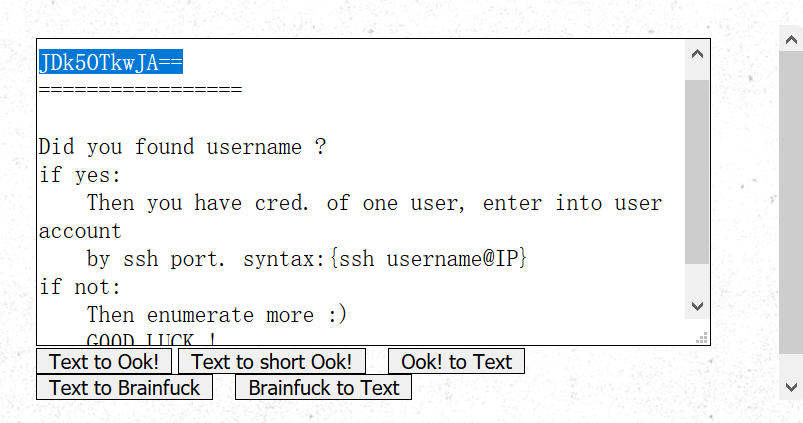
跟进以后F12一波又是加密



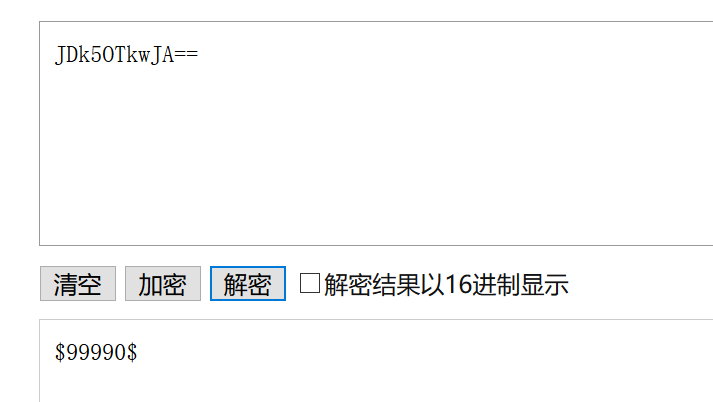
这里查了下可以用Brainfuck解释器转回去



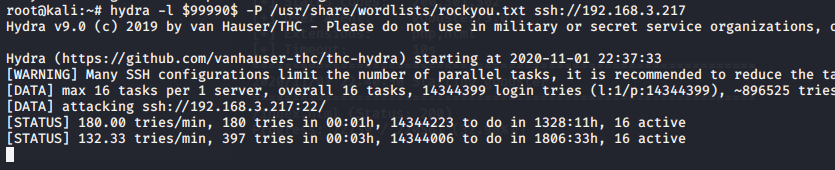
解码以后终于得到想要的文本了，同时得到另外一串加密字符



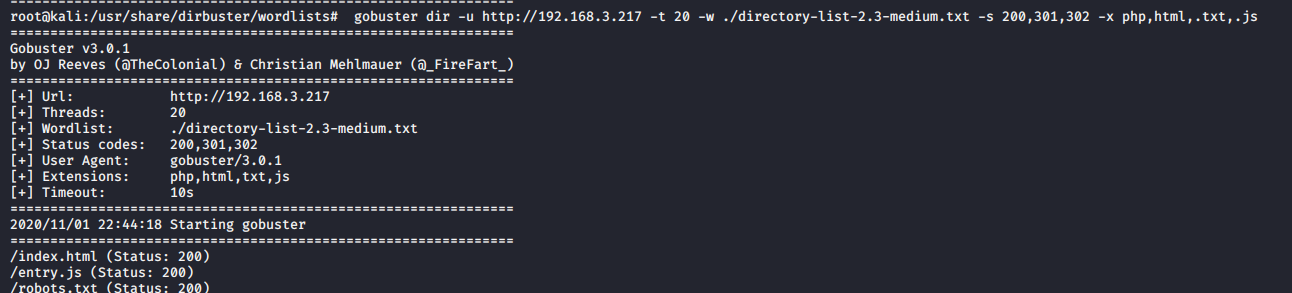
继续解emmm账号是$99990$?????



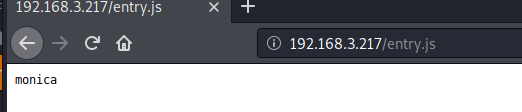
这里我的想法是先丢到hydra爆破一波



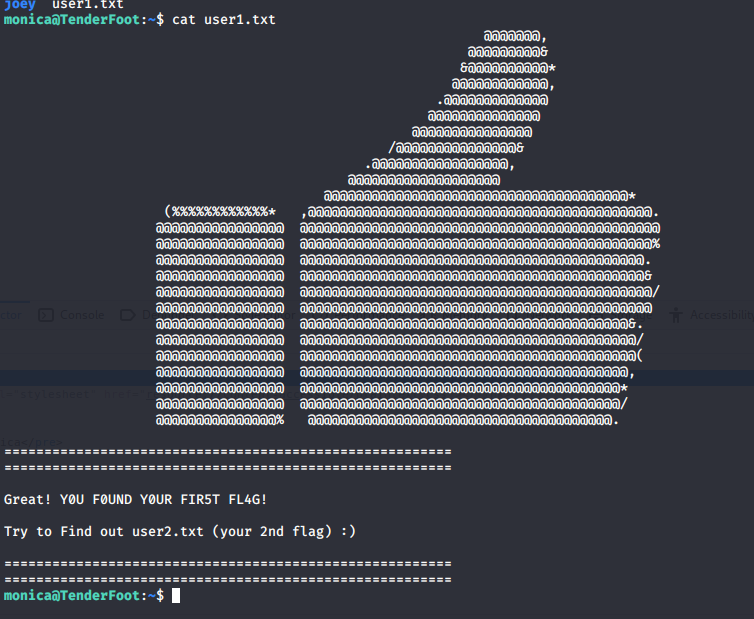
然后再用gobuster加各种常见后缀，终于扫出了一个/entry.js出来



跟进以后第一想法是hydra加入monica爆破

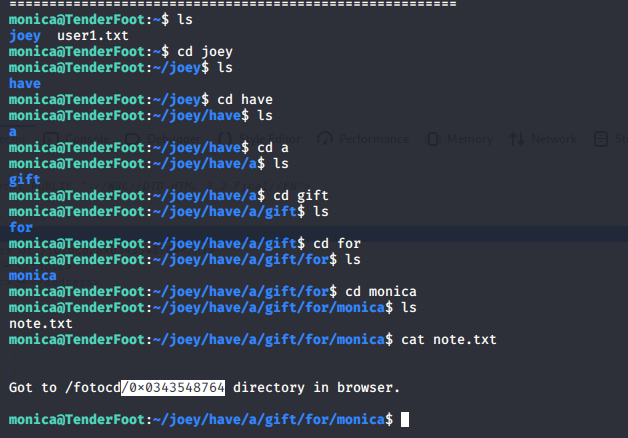


然而还是太年轻了，只需要monica + $99990$就能登录成功了，花了好久专注爆破。。。顺便得到第一个flag

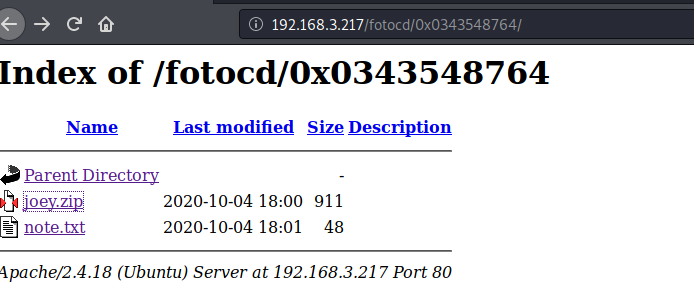


# 0x03:二次挖掘信息

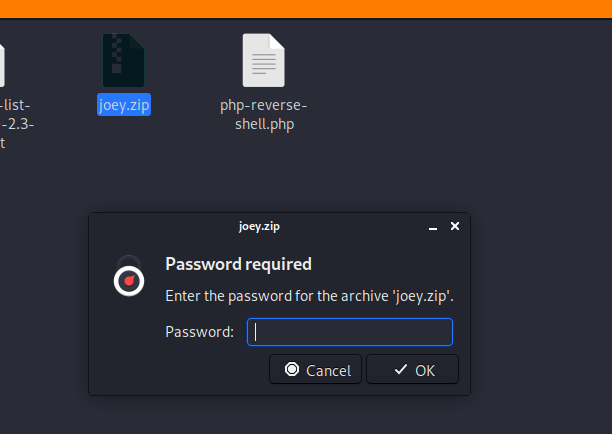
然后查看了下有个joey的目录，经历了几次套娃以后让我们去回/fotocd/目录下还有另外一个目录



跟进以后有个.zip的文件

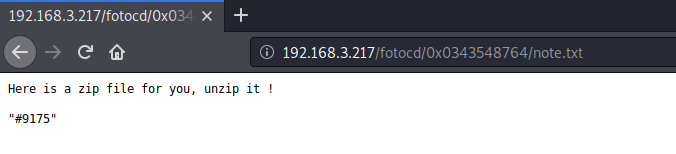


不过下载以后有密码

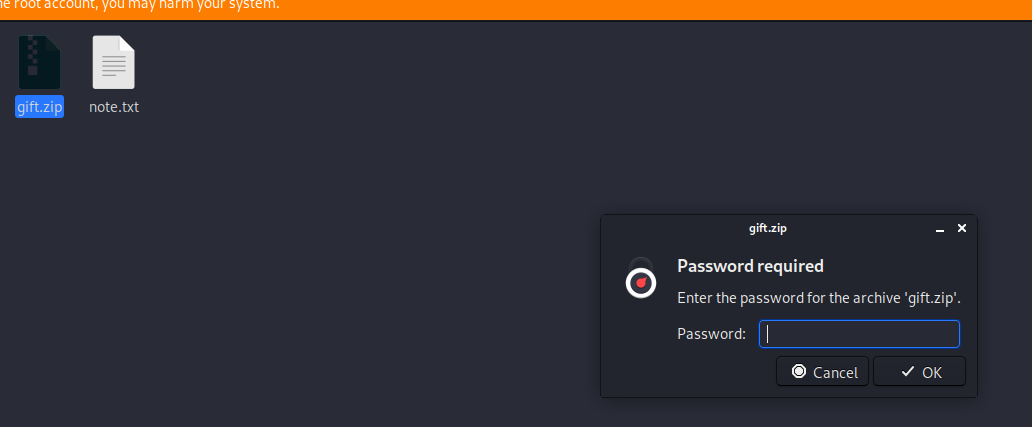


# 0x04:利用John破解密码

这里先别那么憨憨直接冲过去就解了，打开了以下Note.txt发现是可以解joey.zip的



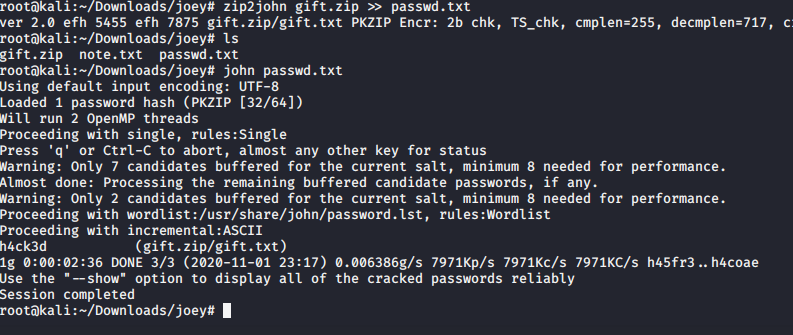
然后里面有个gift.zip需要用到John爆破



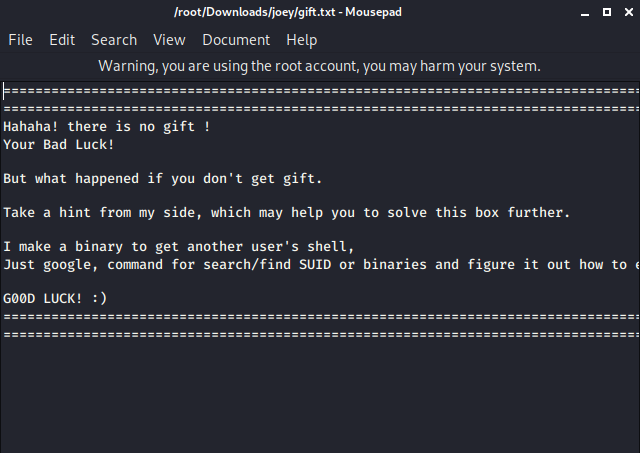
在网上查了一波用John爆破的方法https://www.cnblogs.com/despotic/p/11344141.html



成功得到密码

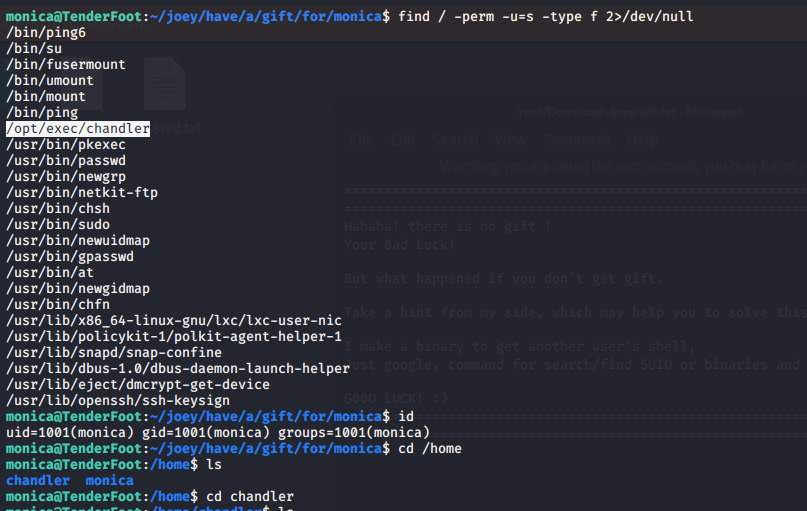


只不过打开以后快要脑淤血了。。。。。。。。

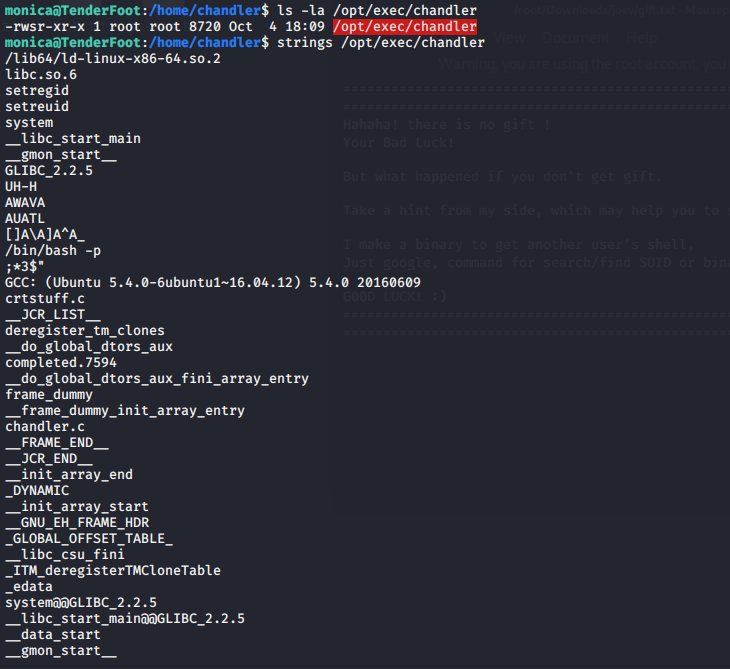


# 0x05:三次挖掘

这里提示说有个二进制的文件是另外一个User的shell来的这里用find 找到了一个/opt/exec/chandler的文件，然而chandler是个用户来的



跟进了以下是个二进制的文件

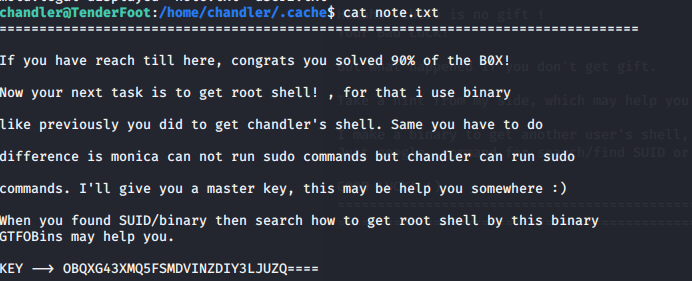


直接运行了一波变成chandler了，然后在.cache目录下得到第二个flag



# 0x06:提权

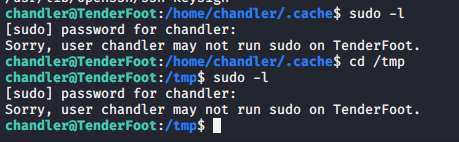
这里在cat note.txt发现了一串key然后拿去解密以下

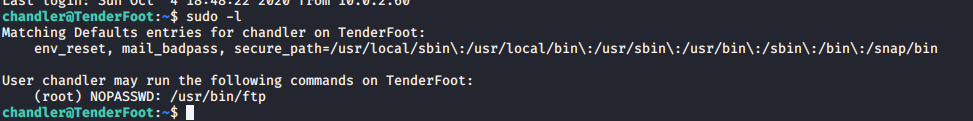


用了base32解密以后得到一串密码

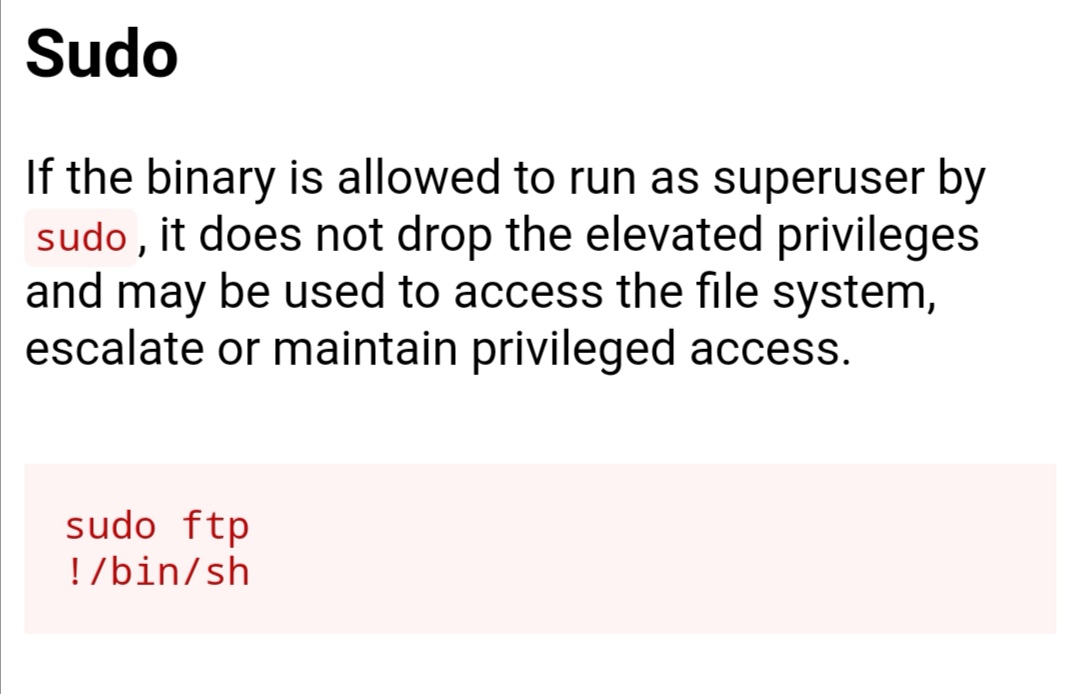


一开始我以为是root的密码，行吧。。。。原来只是chandler的密码，只是奇怪的是目前直接用sudo -l没权限，但是用ssh再次登录以后就有权限了我也不知道为啥





ftp提权还是简单的



只需要按照上面的步骤就能获得root权限了。做完以后真的感觉一定要心平气和

