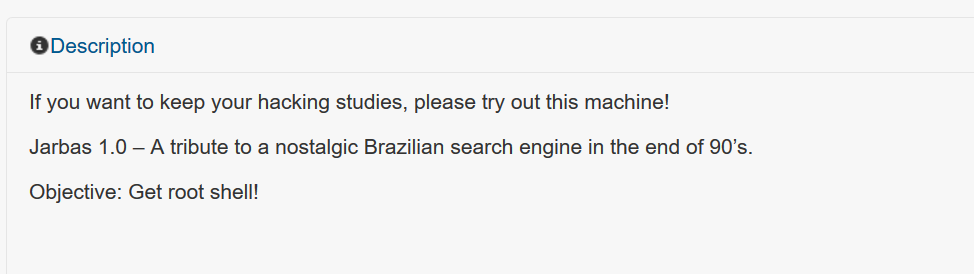
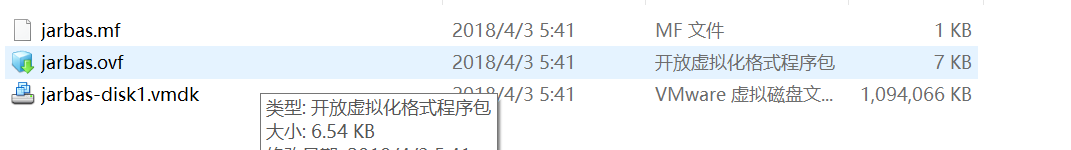
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/jarbas-1,232/>

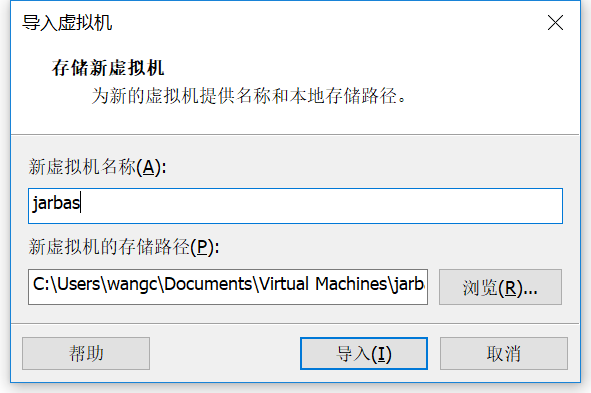
看了一下目标是获取root权限



下载完以后点解压，点击jarbas.ovf开始安装



这里选择一个空目录进行安装



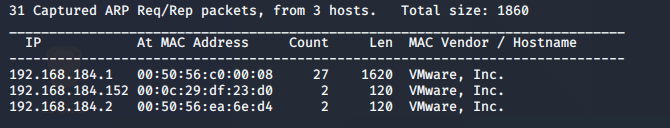
安装好以后是默认调到NAT模式不用重新再弄一次，直接打开就行了



# 0x01:探测靶机

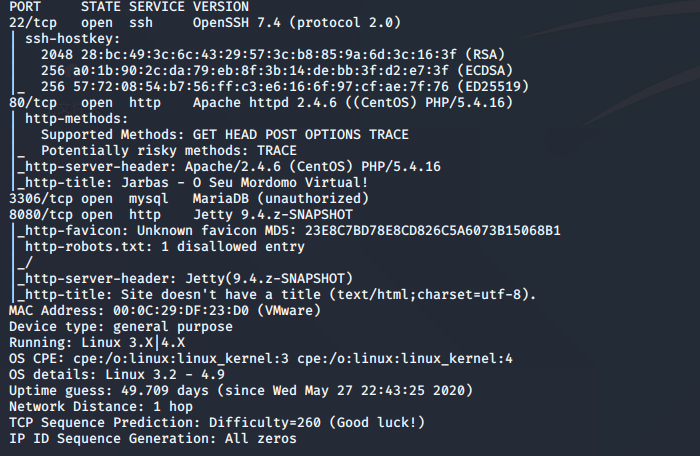
先用netdiscover发现靶机ip排除.1,.2默认网关可以确认靶机IP为192.168.184.152

命令:netdiscover -r 192.168.184.152

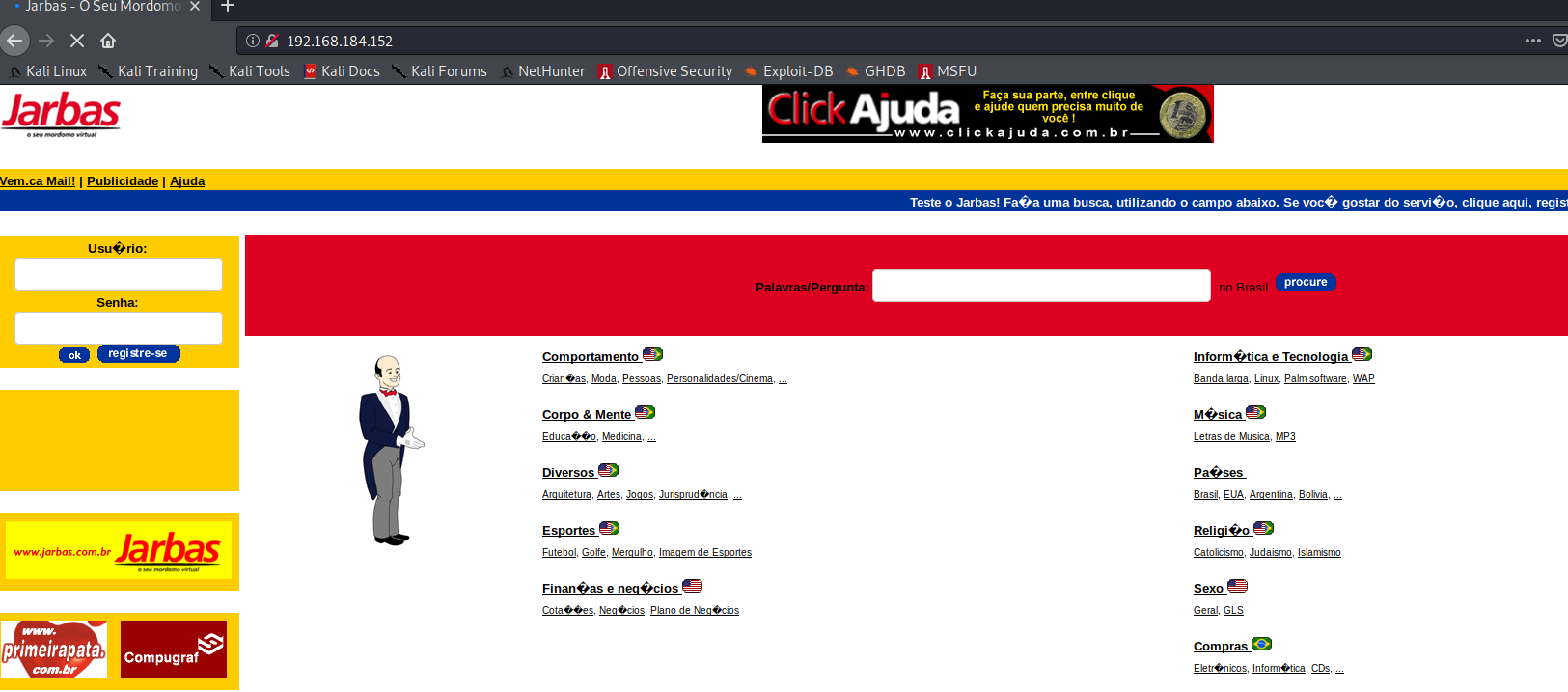


开始用nmap探测端口，主要开了22，80，3306和8080

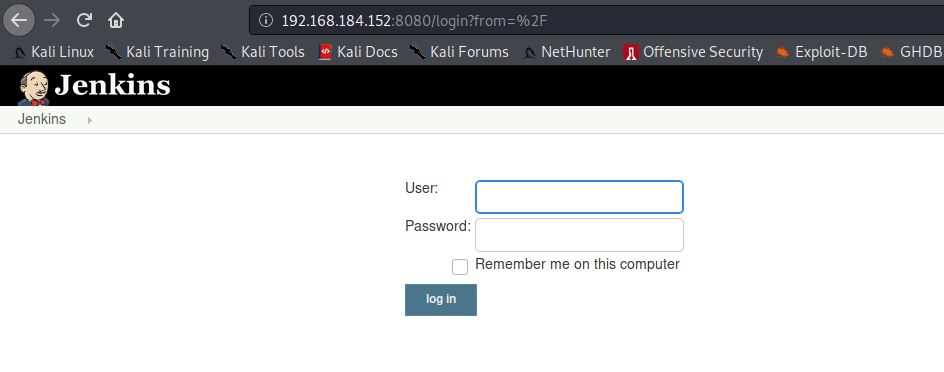
命令:nmap -A -sS -sV -v -p- 192.168.184.152



查看一下页面发现可以正常访问80端口

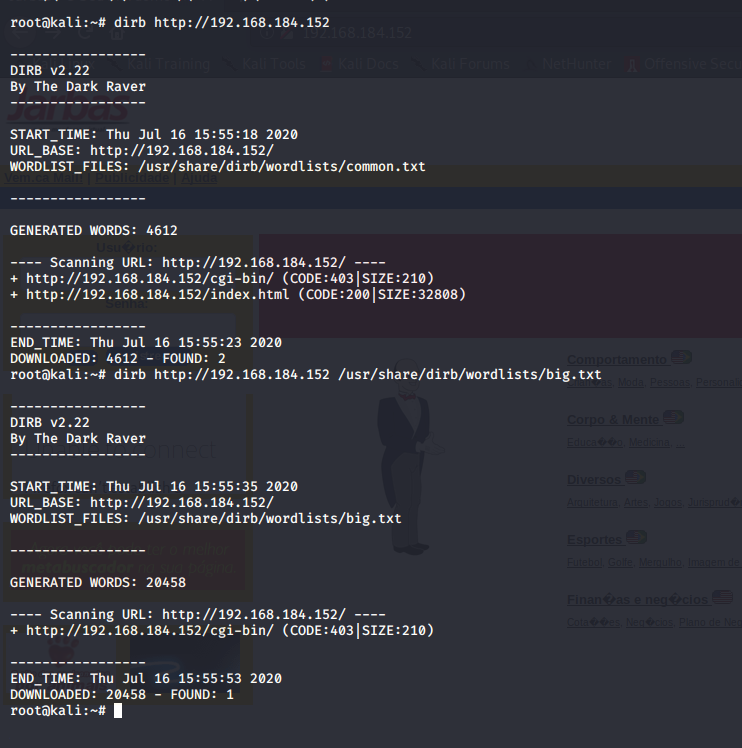


8080端口是一个登录页面，其余端口暂时用不上

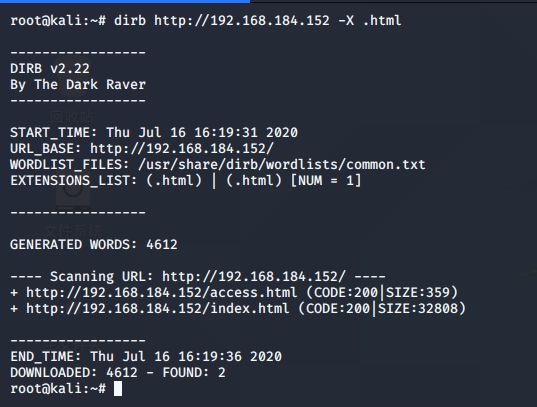


# 0x02:挖掘漏洞

这里尝试一波目录挖掘，用dirb加载两个字典都没发现比较多的信息



换个参数 -X可以理解为加强版在每个测试目录加上后缀扫出一个access.html的网页

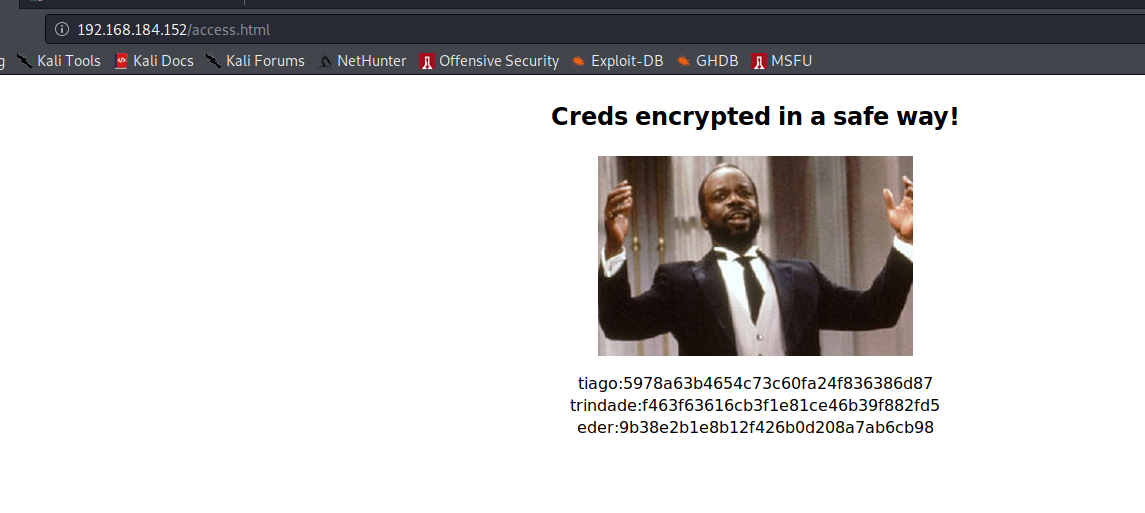


访问以后似乎是一些账号密码最后用在线解密跑出来账号密码为

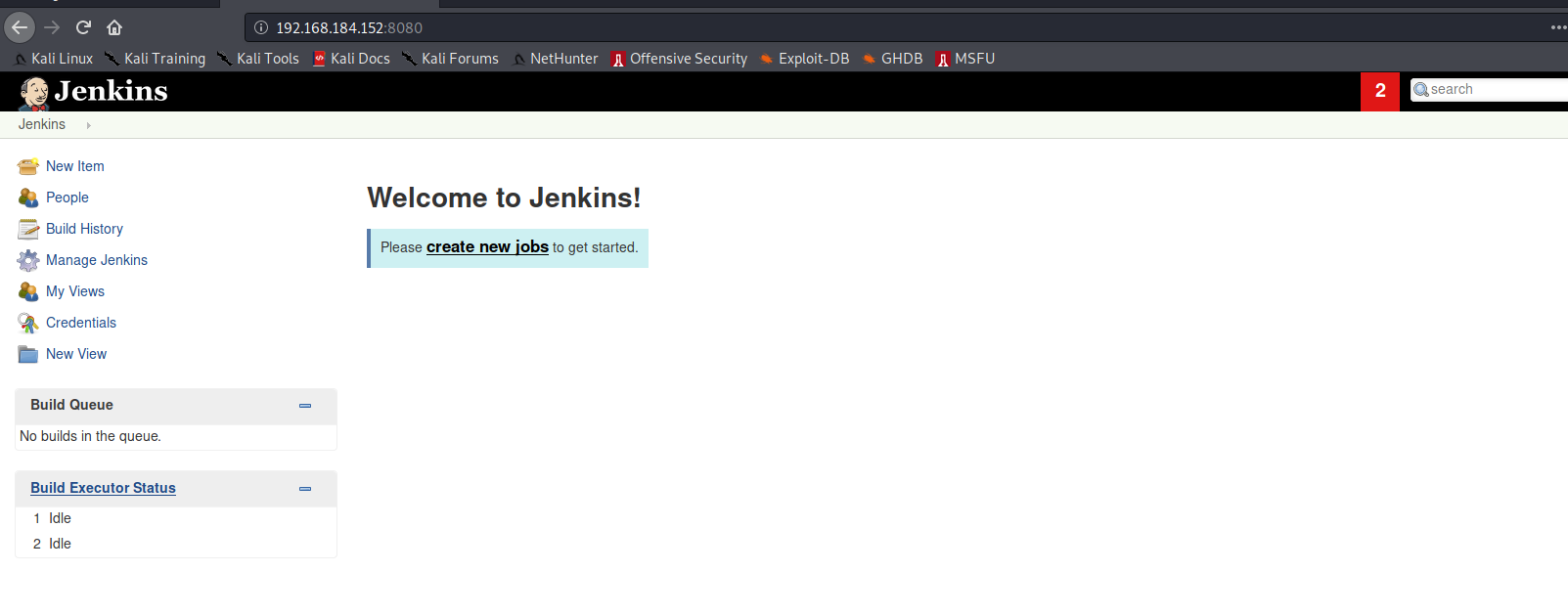
Tiago:italia99

Trindade:marianna

Eder:vipsu

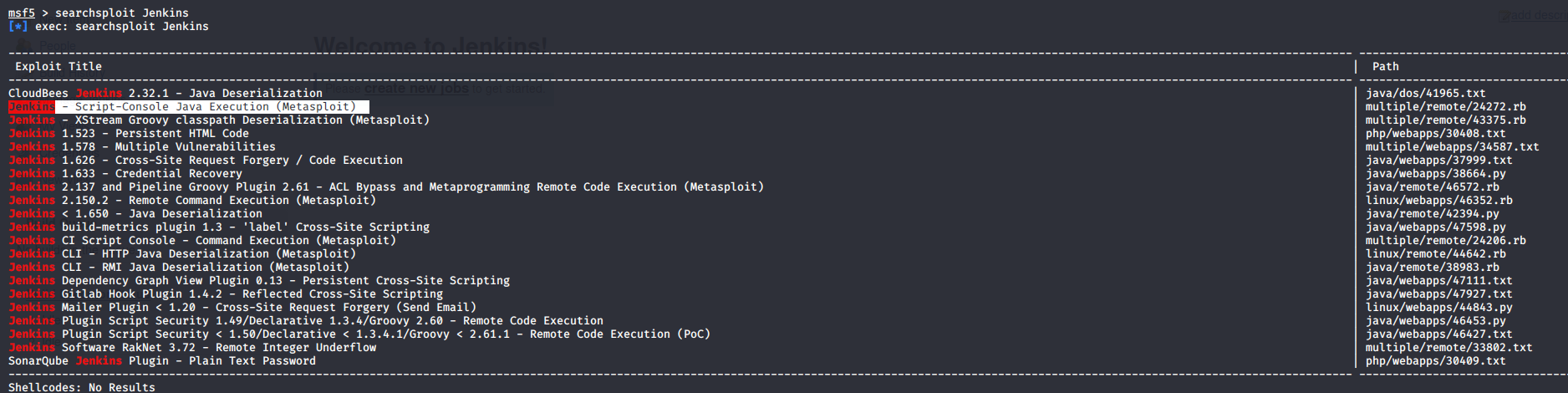


尝试用这些账号登录22端口卒，去到8080端口用eder的账号密码才能成功登陆

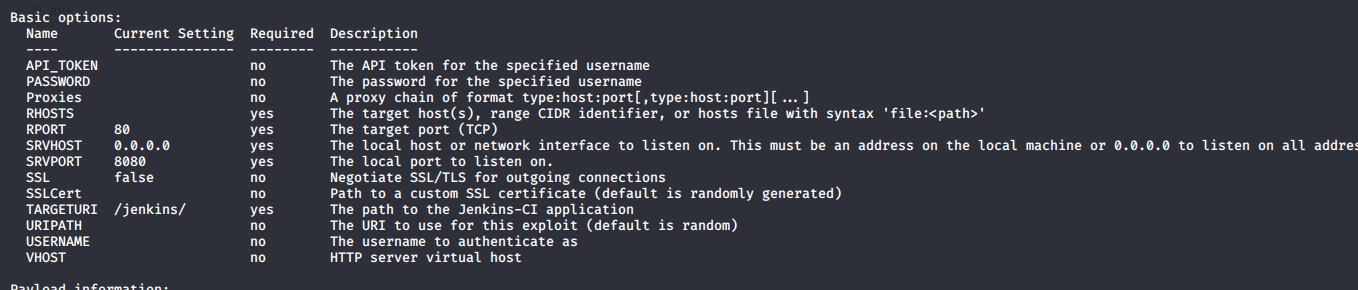


# 0x03:MSF获取shell

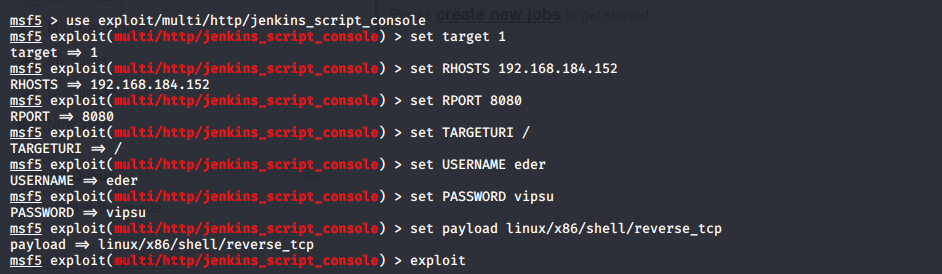
用MSF搜索刚才登录进去大大的Jenkins真的发现有payload可以利用

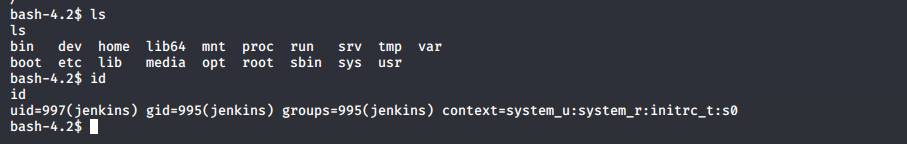


这里我选择exploit/multi/http/jenkins\_script\_console payload先查看下要填的东西为RHOST(目标ip) ,RPORT（目标端口）,TARGETURI（位置） 顺便填一下用户名和密码，然而这个payload只能执行命令执行还需要配合一个Linux的反弹shell来获取shell



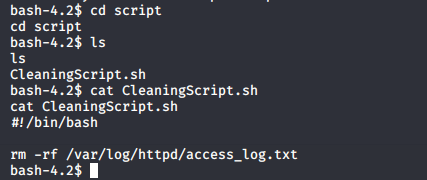
开始启用，并获得shell



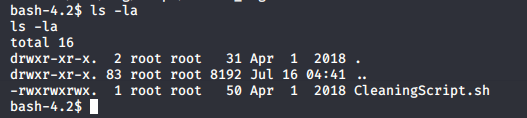


# 0x04:提权

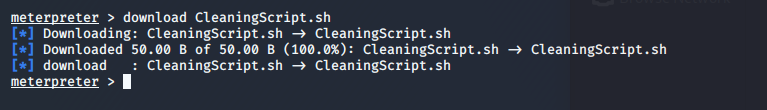
由于是靠反弹得到的shell目前不知道密码先逛该在/etc/script目录下有个特别的文件CleaningScript.sh查看一下是个跑路命令rm -rf 删除文件如果是星号就是真的跑路了



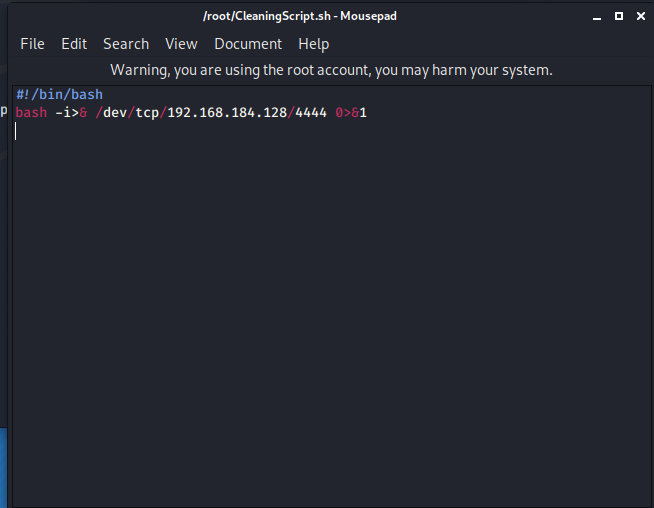
同时查看权限是root



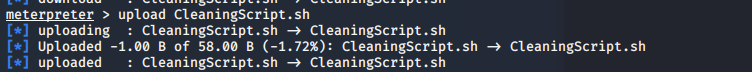
这里有个想法，先下载CleaningScript.sh文件，然后更改里面的内容把里面的东西换成一个反弹shell，最后在重新上传提前开启netcat获得另外一个shell ，这里由于kali崩了一下换了另外一个kali没有加反弹shell



下完以后加入一个反弹shell



传回去



提前开启netcat成功得到root权限

