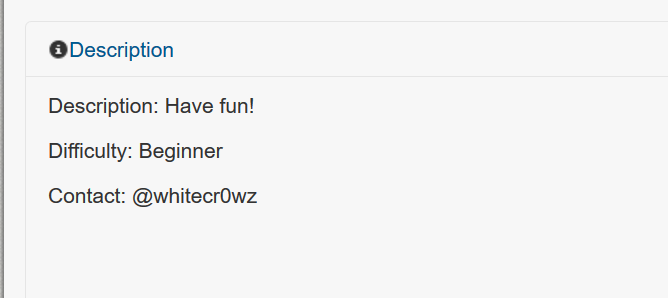
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/sunset-sunrise,406/>

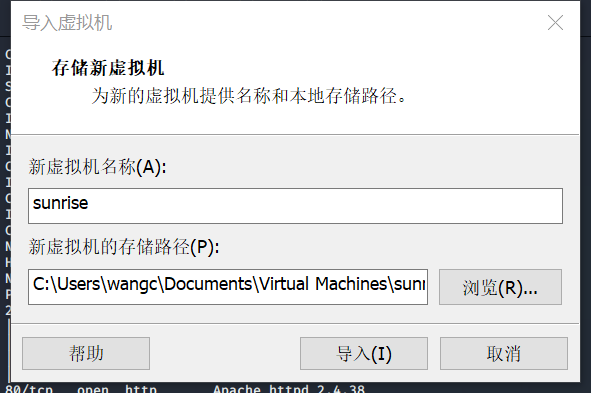
描述过于简单。。。。。。



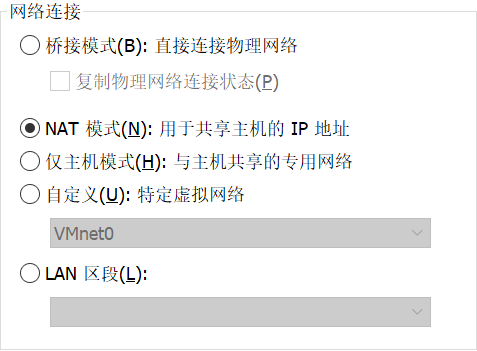
下载解压好以后是个.ova文件，可以选择用VM或者是VirtualBox进行安装，这里我选择VM



双击以后选择一个合适的地方进行存放即可



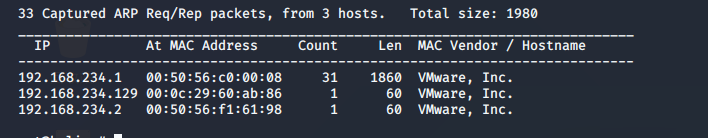
安装好以后记得把网络模式调回NAT否则获取不了IP



# 0x01:探测靶机

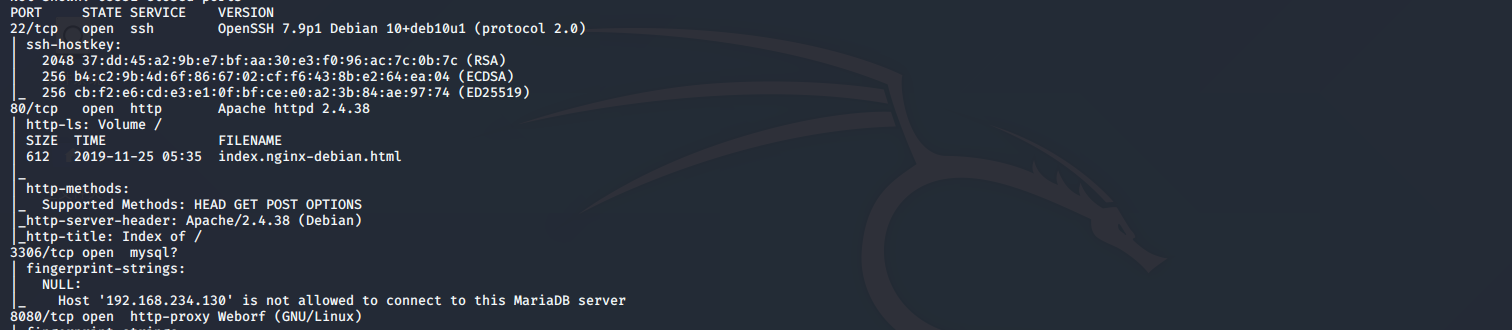
还是先用netdiscover探测一波,排除.1,.2默认网关可以确认靶机IP为192.168.234.129

命令:netdiscover -r 192.168.234.0/16

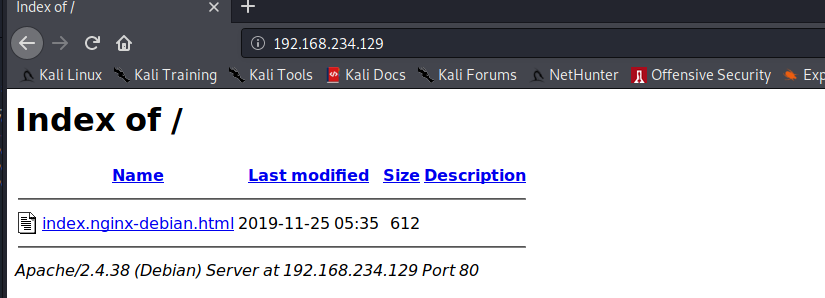


接下来就是用nmap探测一波端口，开了22，80，3306和8080端口

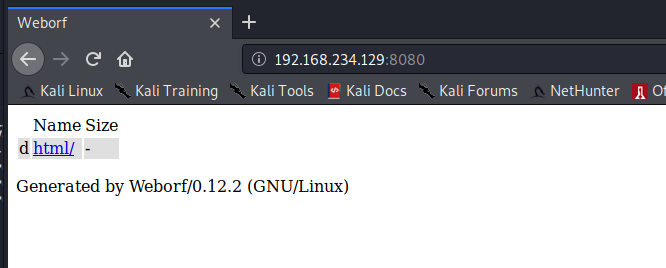
命令:nmap -A -sS -sV -v -p- 192.168.234.129



先正常访问一波80和8080端口看看能不能正常访问



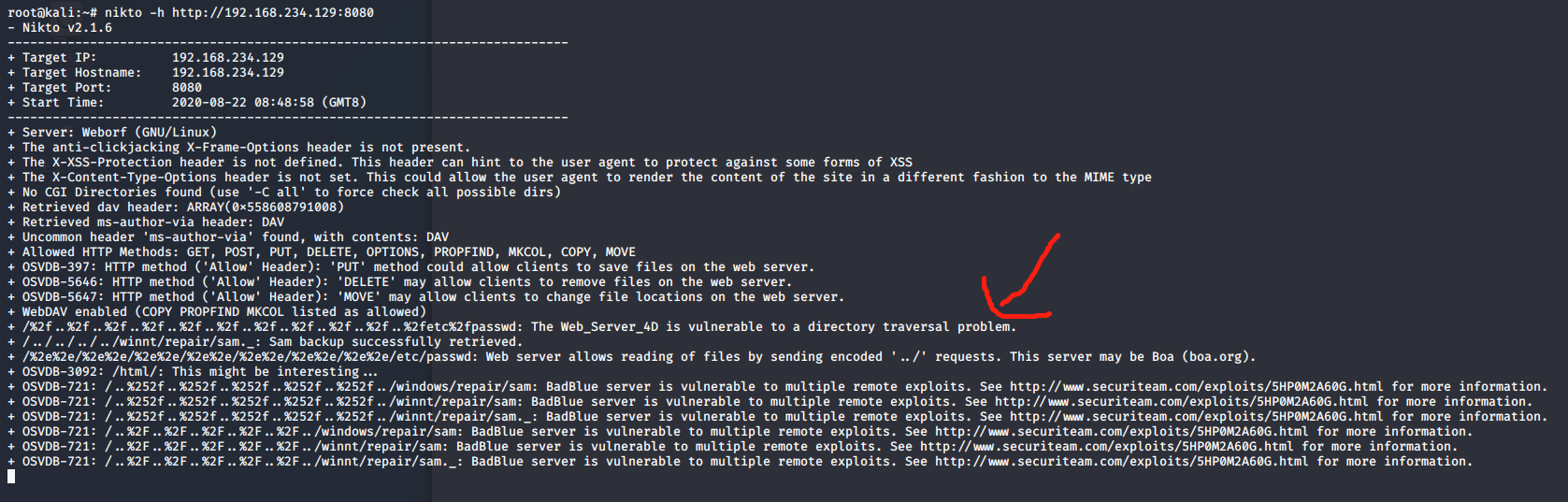
80和8080端口都是页面回显信息比较少只能用dirb和nikto看看能挖掘什么东西出来



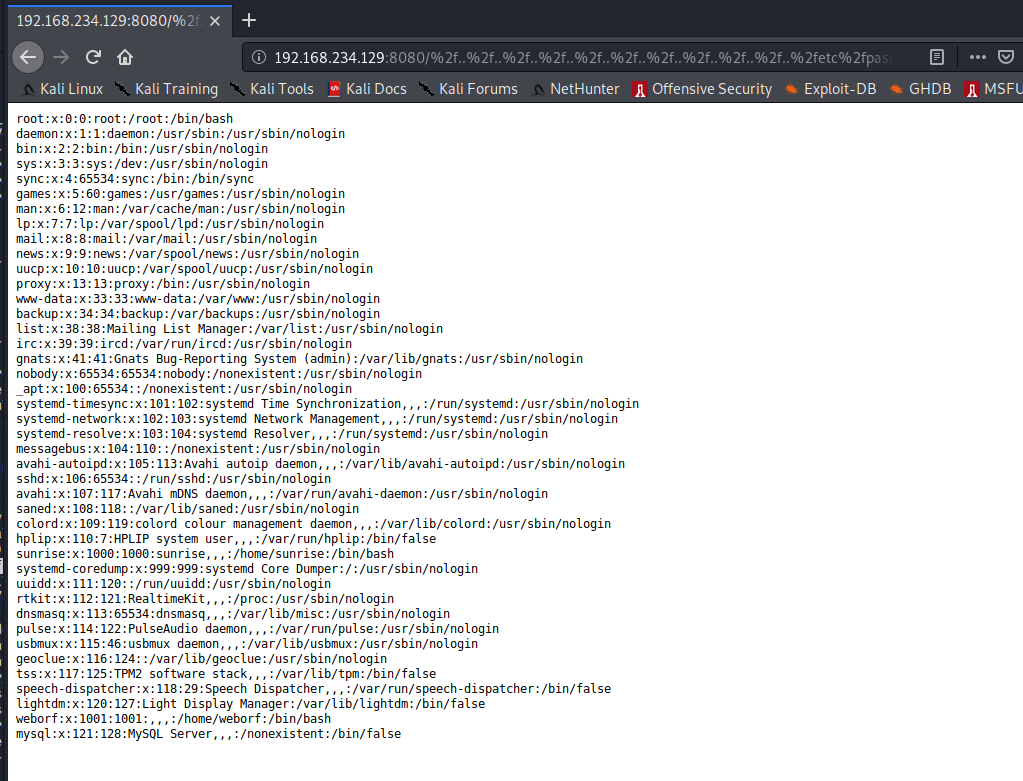
# 0x02:挖掘漏洞

再用Nikto扫8080端口的时候已经可以扫到有一个目录穿越漏洞并顺便附上payload出来

Payload: /%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd

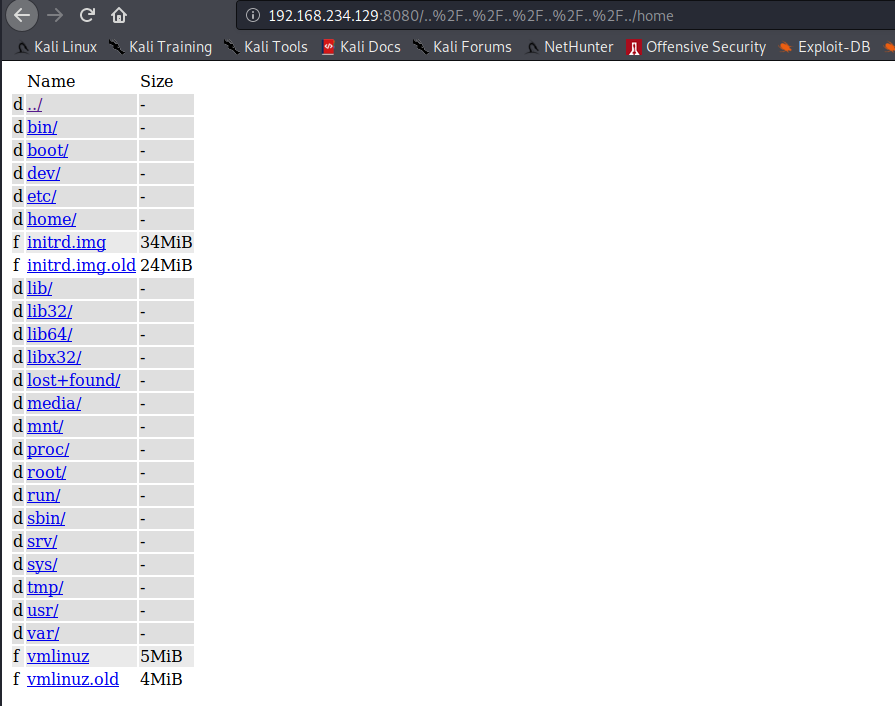


跟进一下是可以读取到当前的账户名字信息

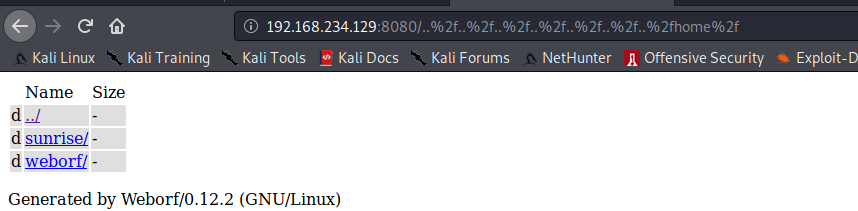


# 0x03:目录穿越漏洞

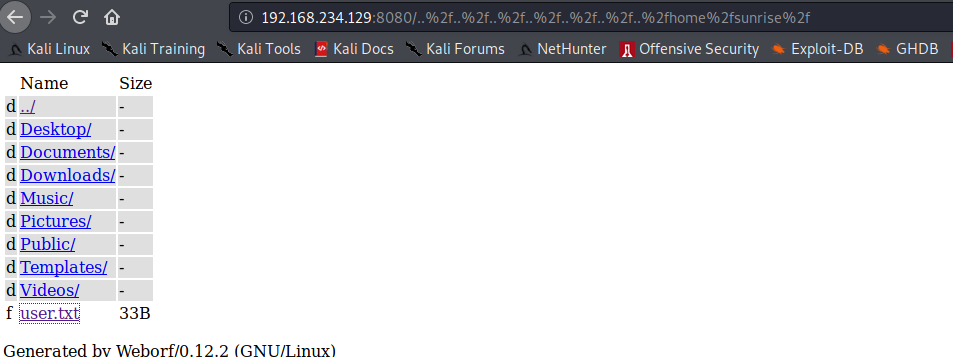
再跟进另外一个payload可以看到跟目录下的文件夹有哪些

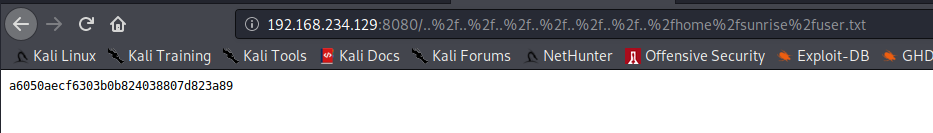


尝试进入到hone目录下，发现有2个用户这里选择sunrise看看里面的东西

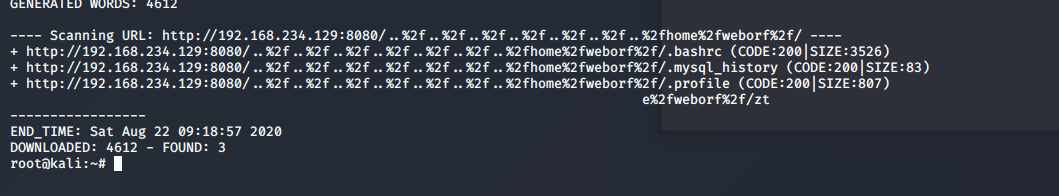


进入到sunrise以后有个user.txt可以读取到里面的内容，应该是user的flag

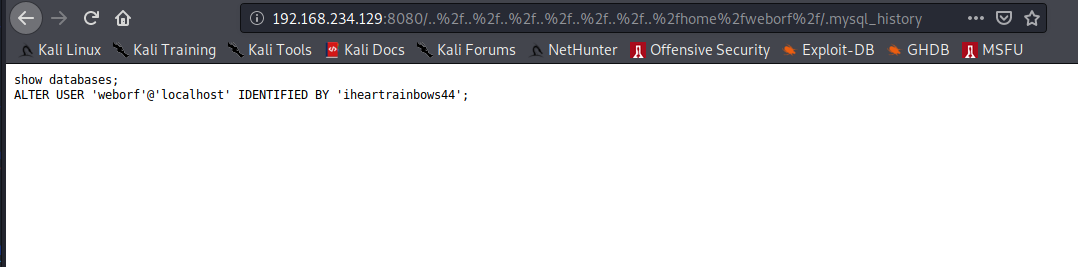




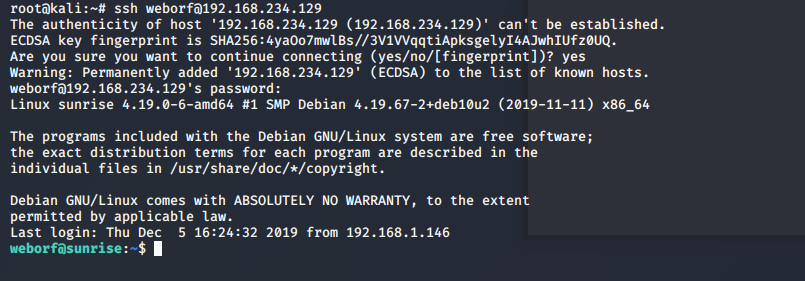
然后去回weborf里面看看然而没有东西，只能用dirb可以扫出3个东西出来



逐一查看以后发现.mysql\_history有账号密码回显



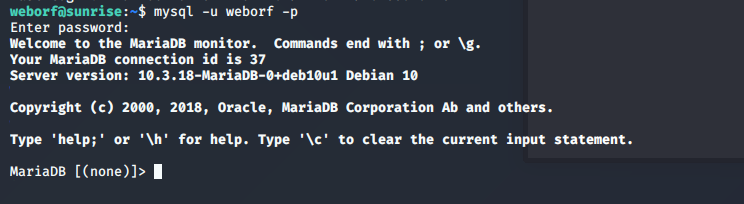
利用该账号可以成功登录SSH



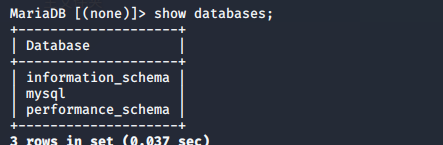
# 0x04:挖掘数据库信息

由于在一开始用nmap探测的时候已经开启了3306的数据库端口这里尝试进入一波挖掘信息

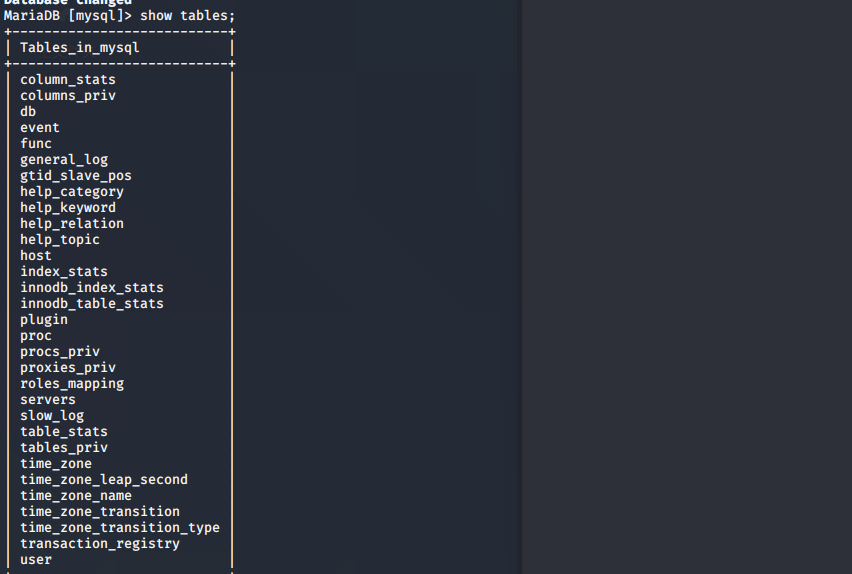
命令:mysql -u weborf -p 进入



看看有哪些数据库，只能选择mysql



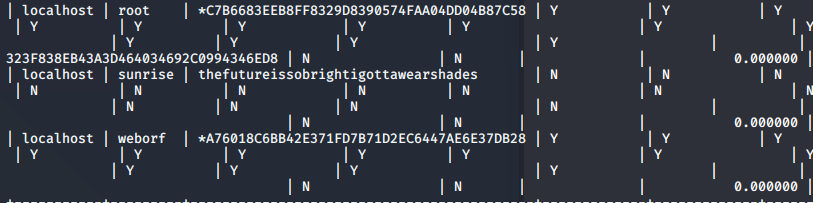
在查看表的时候发现一个关键词user



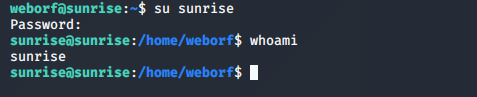
跟进以后除了不美观。。。可以得到3个账号的用户密码信息，然而root的密码根本解不开，

要不然直接root进去拿flag了

Sunrise:thefutureissobrightigottawearsshades

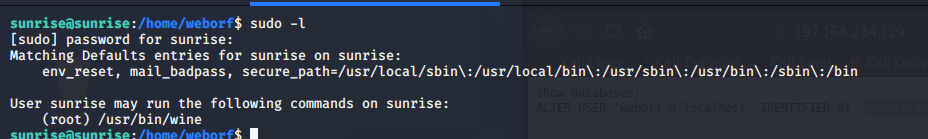


只能切换成sunrise的用户了。。。。。



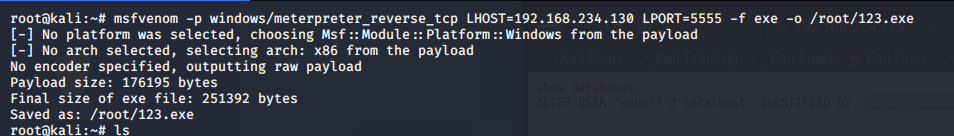
# 0x05:提权

先用sudo -l查看有没有特殊权限结果发现个wine..逐渐感到迷惑



去必应查了查确实可以用wine进行提权，<https://www.hacknos.com/wine-privilege-escalation/>然而这篇文章有个问题是按照他的步骤生成的exe有点问题得稍微更改一下

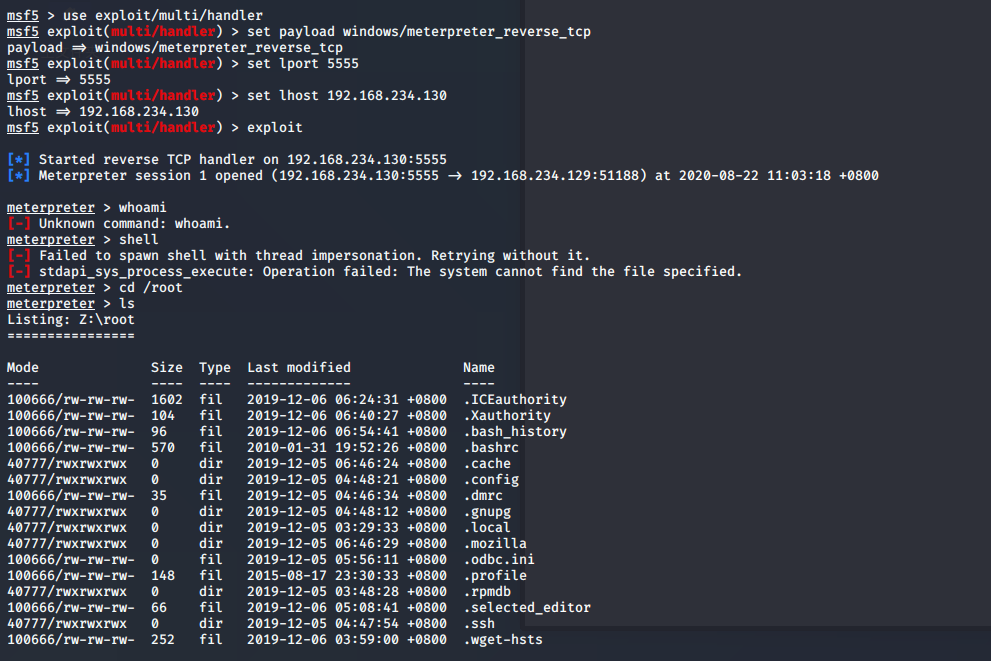
首先用msf生成程序



然后可以用scp或者是python传上去这里我用scp，成功上传



设置好以后进入MSF设置好payload运行就可以得到权限了



然后顺利读到flag

