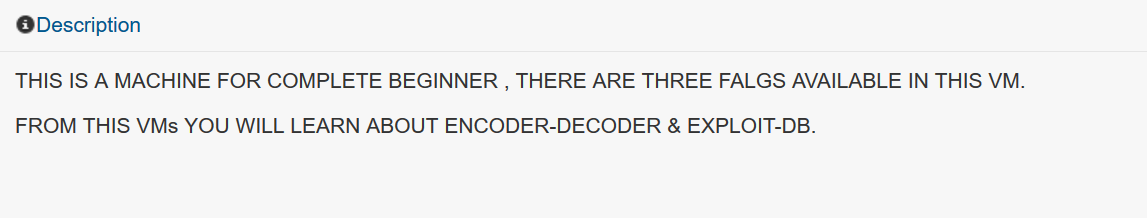
# 0x00:靶机下载:

下载链接: <https://www.vulnhub.com/entry/cybersploit-1,506/>

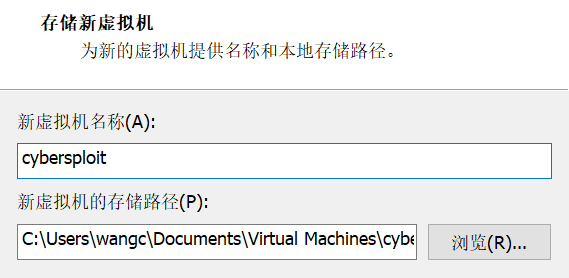
看了一下描述是新手级别，3个flag会用到加密，解密，脚本



下载完以后是个.ova文件



双击，选择一个合适的位置存放



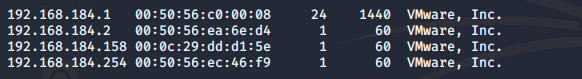
安装好以后，需要调到NAT模式，默认是桥接模式。不一定能获取IP



# 0x01:探测靶机

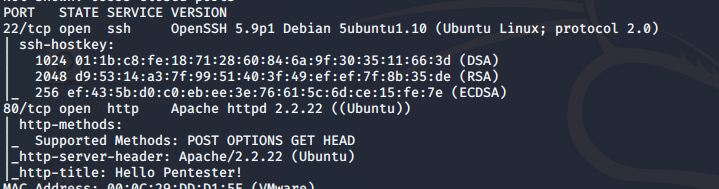
先用netdiscover确认靶机IP，排除.1,.2可以确认靶机IP为192.168.184.158

命令:netdiscover -r 192.168.184.0/16



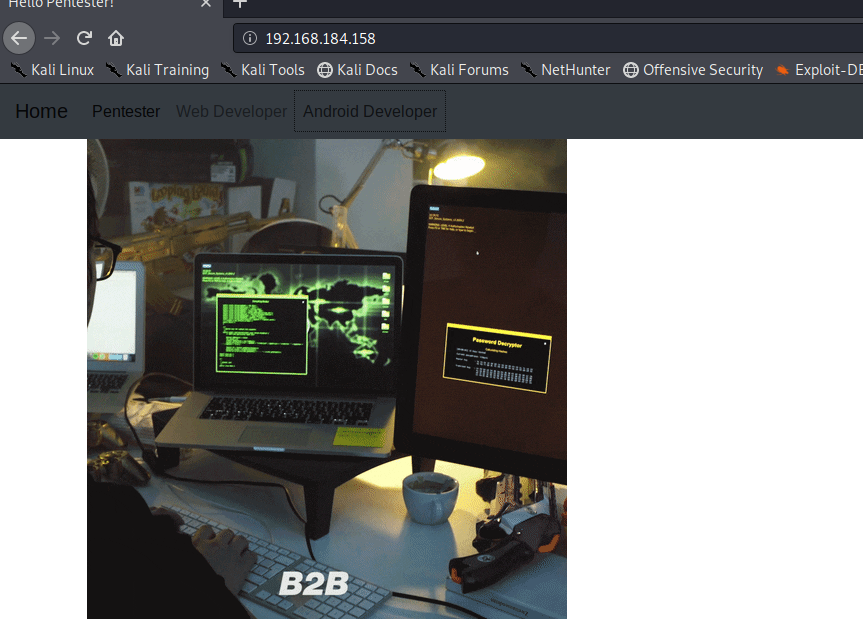
开始用nmap探测端口,可以看到开了22和80端口，由于目前没收集到啥信息，只能集中在80端口

命令:nmap -A -sS -sV -v -p- 192.168.184.158

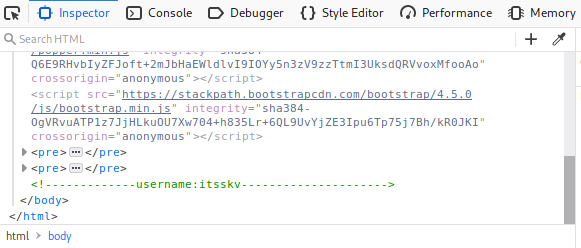


# 0x02:挖掘信息

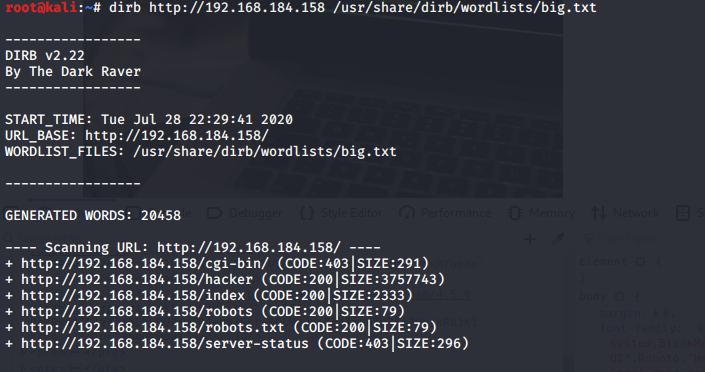
先正常访问一下IP地址，可以正常回显，虽然有几个分页，但是都是一样的动图。。。。。



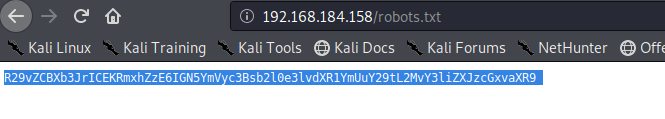
在首页按住F12浏览的时候发现一个username: itsskv记录一下



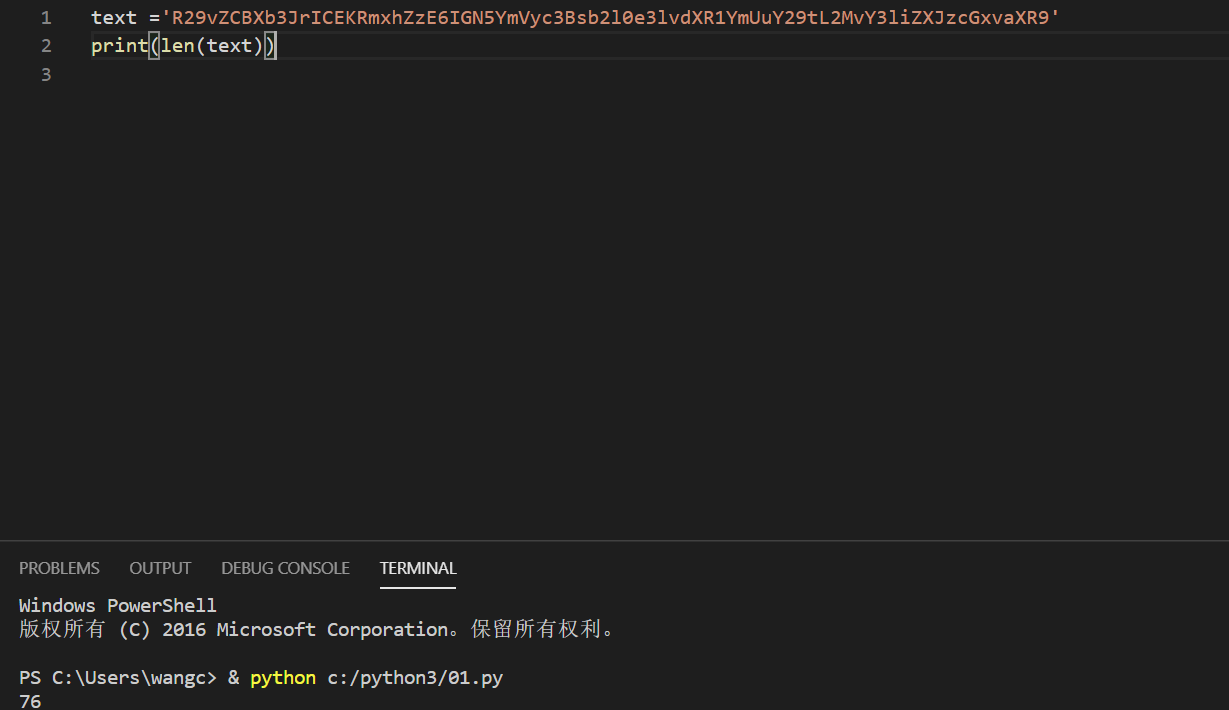
开始用dirb,挖掘目录，发现有robots



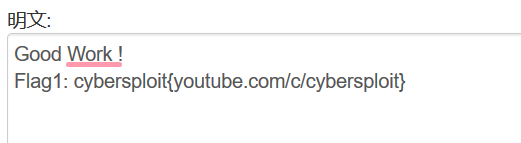
跟进/robots.txt,发现一串字符串不知道啥加密



这里我先用python获取一下长度为76，76可以整除4，可以确定为base64加密

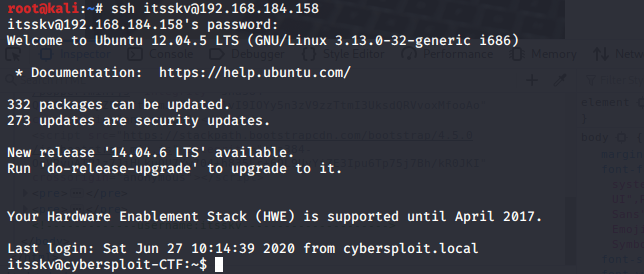


解密以后得到第一个flag



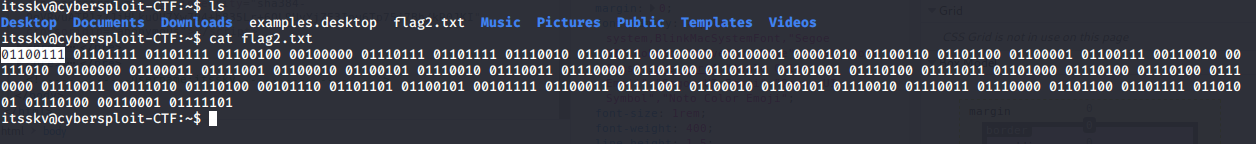
# 0x03:登录22端口

由于现在已经知道用户名了，可以尝试猜一下密码，然而密码居然是cybersploit{youtube.com/c/cybersploit}，直接复制flag的内容就行了。。。。。。

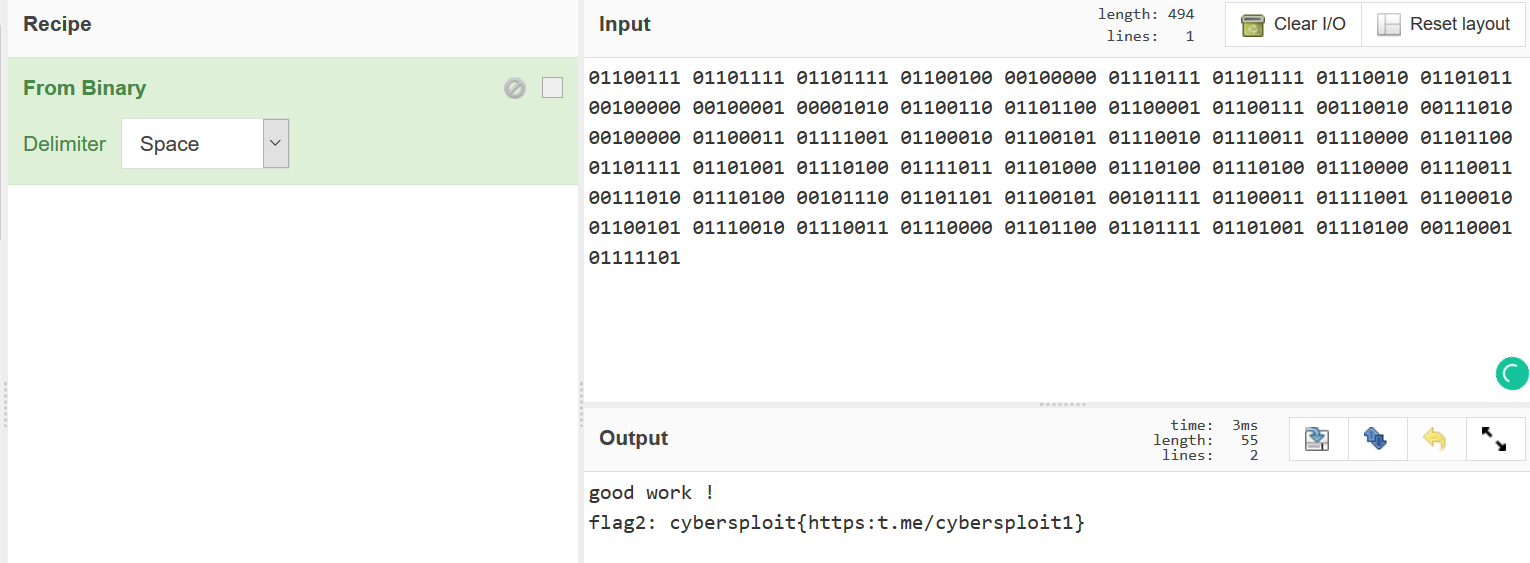


直接ls就发现第二个flag了，这里发现是一串长长的二进制。。。。。不过应该是二进制转字母表这样。如果大家够肝的话可以慢慢手算

01100111 01101111 01101111 01100100 00100000 01110111 01101111 01110010 01101011 00100000 00100001 00001010 01100110 01101100 01100001 01100111 00110010 00111010 00100000 01100011 01111001 01100010 01100101 01110010 01110011 01110000 01101100 01101111 01101001 01110100 01111011 01101000 01110100 01110100 01110000 01110011 00111010 01110100 00101110 01101101 01100101 00101111 01100011 01111001 01100010 01100101 01110010 01110011 01110000 01101100 01101111 01101001 01110100 00110001 01111101



这里用cyberchef解码得到第二个flag的内容

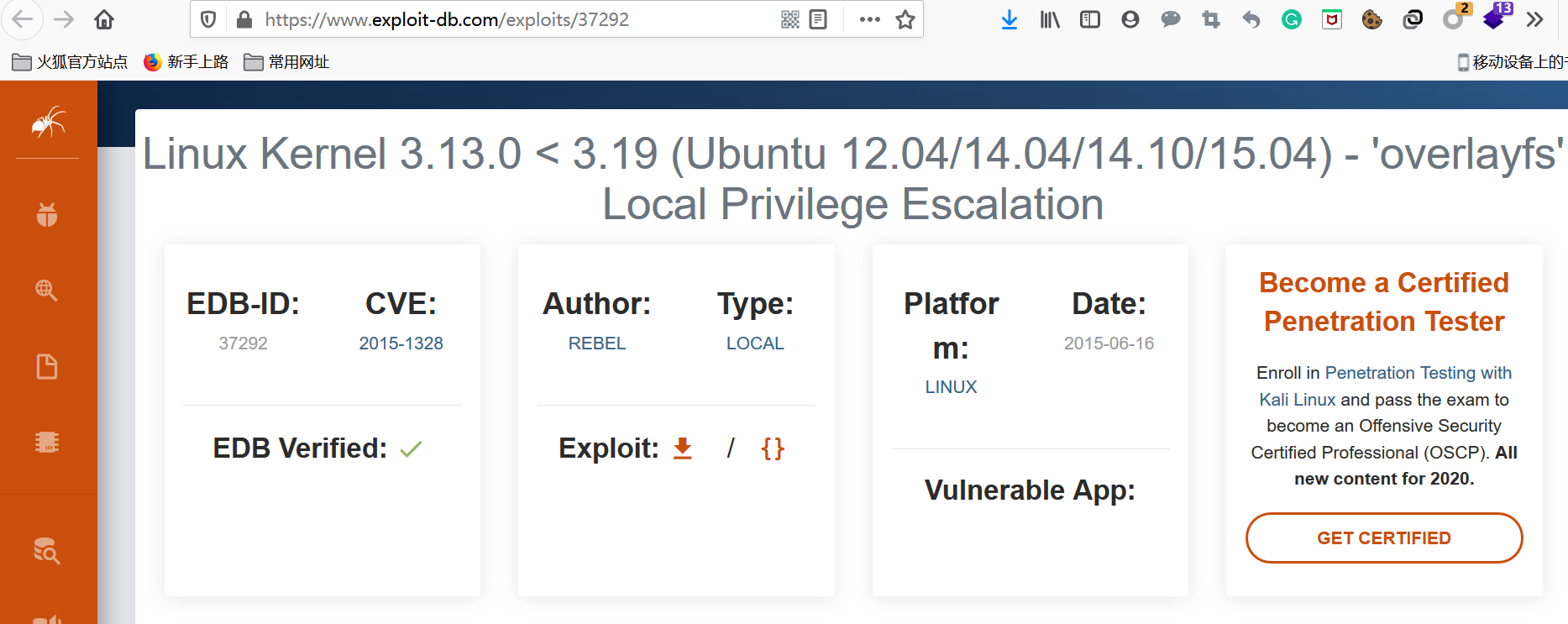


# 0x04:提权

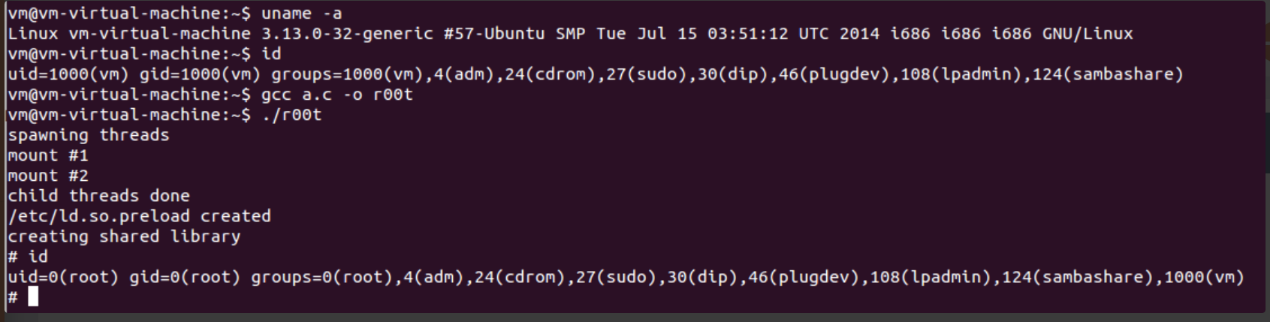
首先先用uname -a查看一下内核先



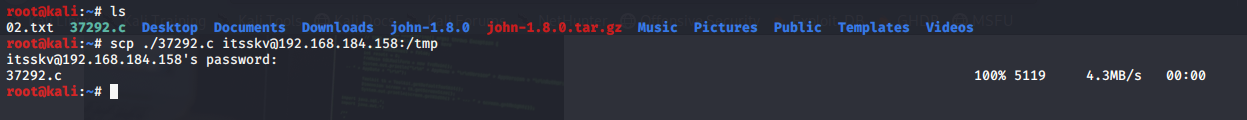
复制关键词，在EXDB找到一个payload



在最底下有一个使用方法



下载完以后用scp命令传到目标服务器上





按照图片的步骤成功得到flag

