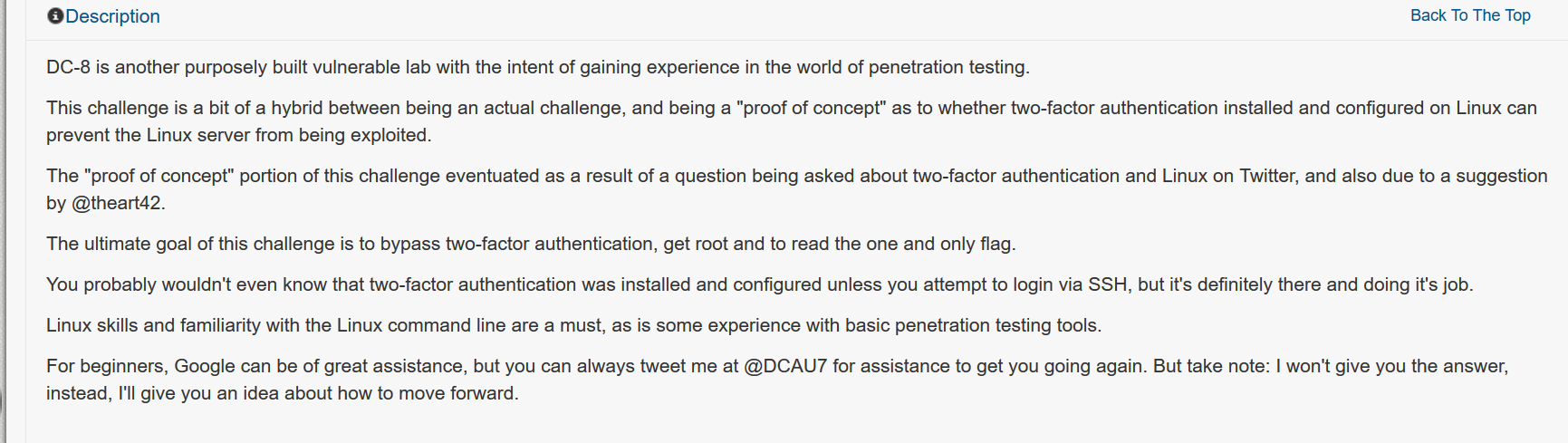
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/dc-8,367/>

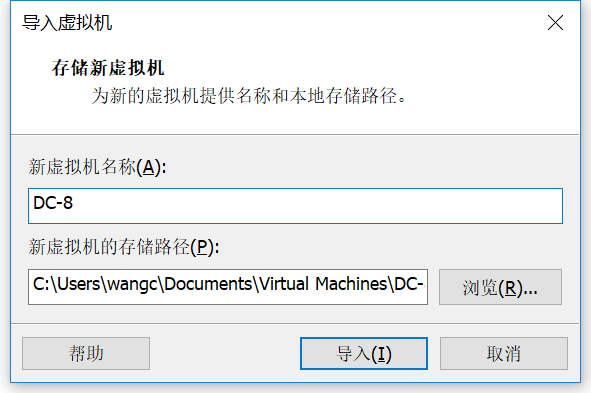


难度可能为中目标是拿到root权限并顺便读取其目录下的flag

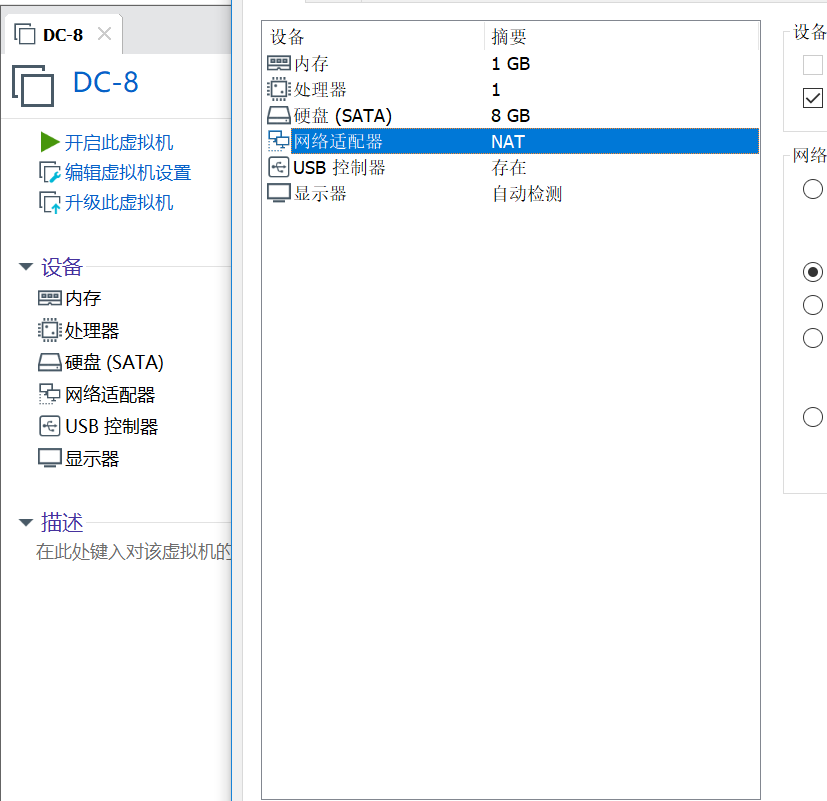
下载完以后是个zip格式解压以后会看到这个ova文件



点击以后选择一个合适的位置即可

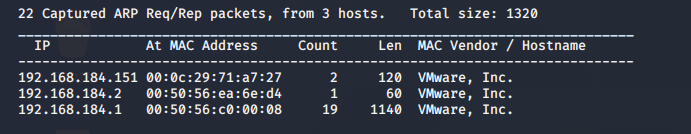


要注意的是该靶机默认的网络连接方式是桥接模式所以需要把它调到NAT模式下



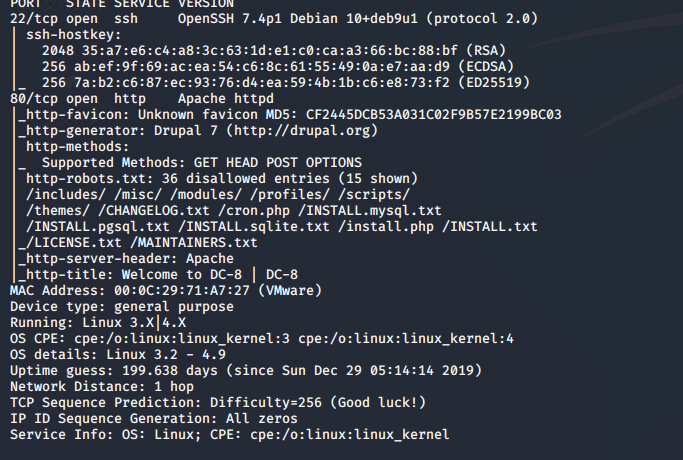
# 0x01:探测靶机

先用netdiscover，排除.1,.2默认网关可以确认靶机IP为192.168.184.151



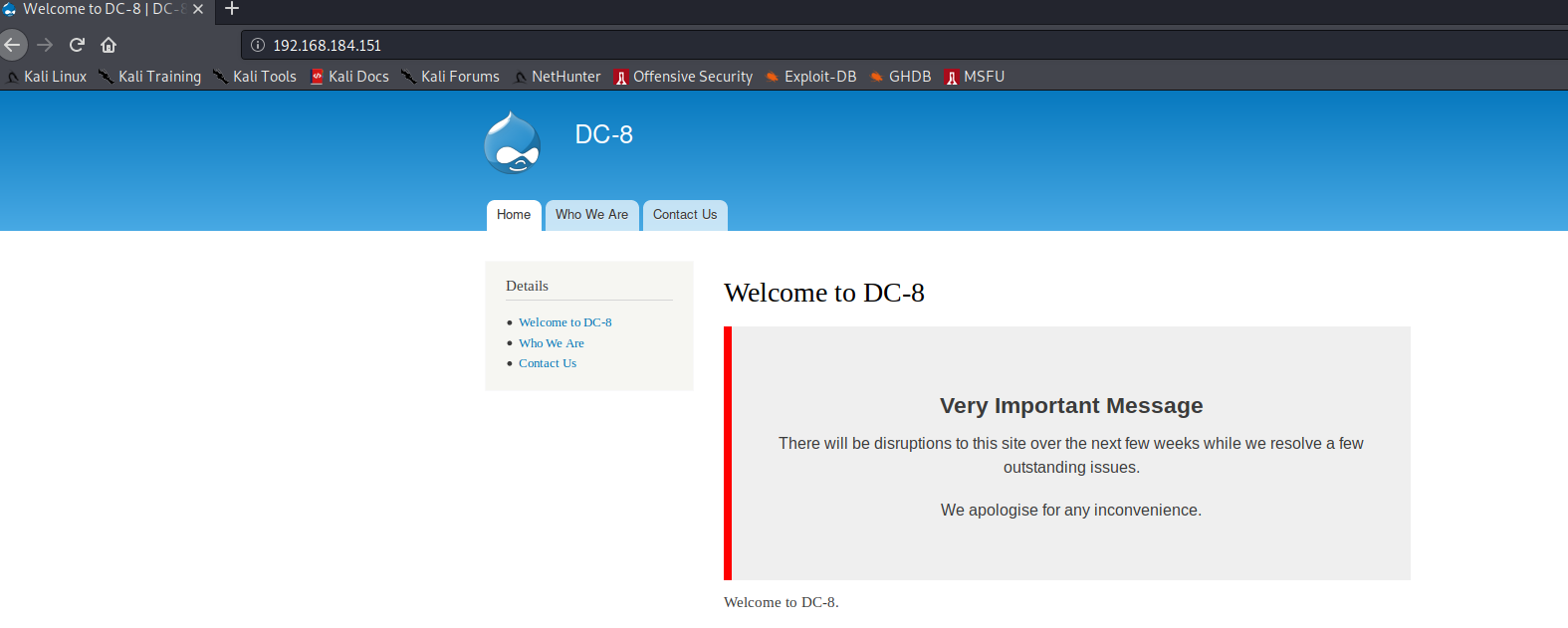
接下来就用Nmap探测端口主要开了22和80

命令:nmap -A -sS -sV -v -p- 192.168.184.151

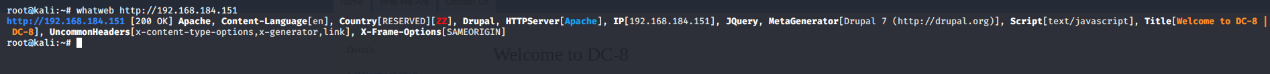


# 0x02:挖掘漏洞

访问一下IP可以正常访问，这个水滴头感觉在很多地方见过



用whatweb看了一下是个Drupal CMS



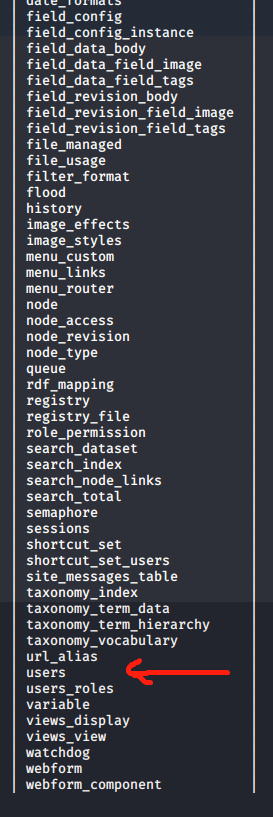
点开其中的链接芜湖直接起飞遇到?nid=1的参数放sqlmap里面



可以直接跑出来



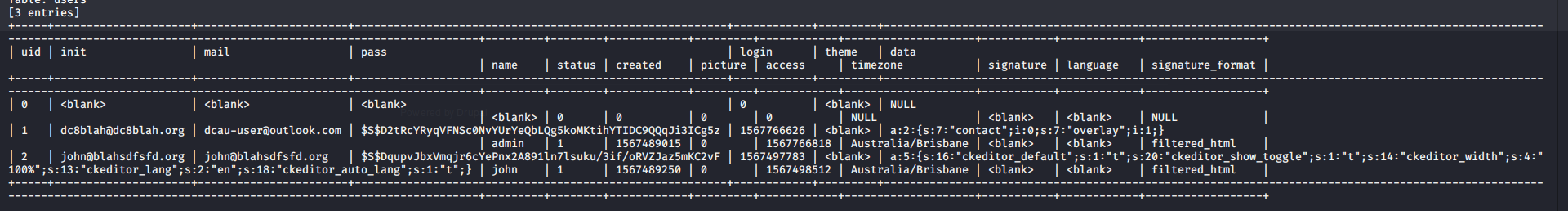
发现关键词user



跑里面的数据最后得到两个账号

Admin $S$D2tRcYRyqVFNSc0NvYUrYeQbLQg5koMKtihYTIDC9QQqJi3ICg5z

John $S$DqupvJbxVmqjr6cYePnx2A891ln7lsuku/3if/oRVZJaz5mKC2vF

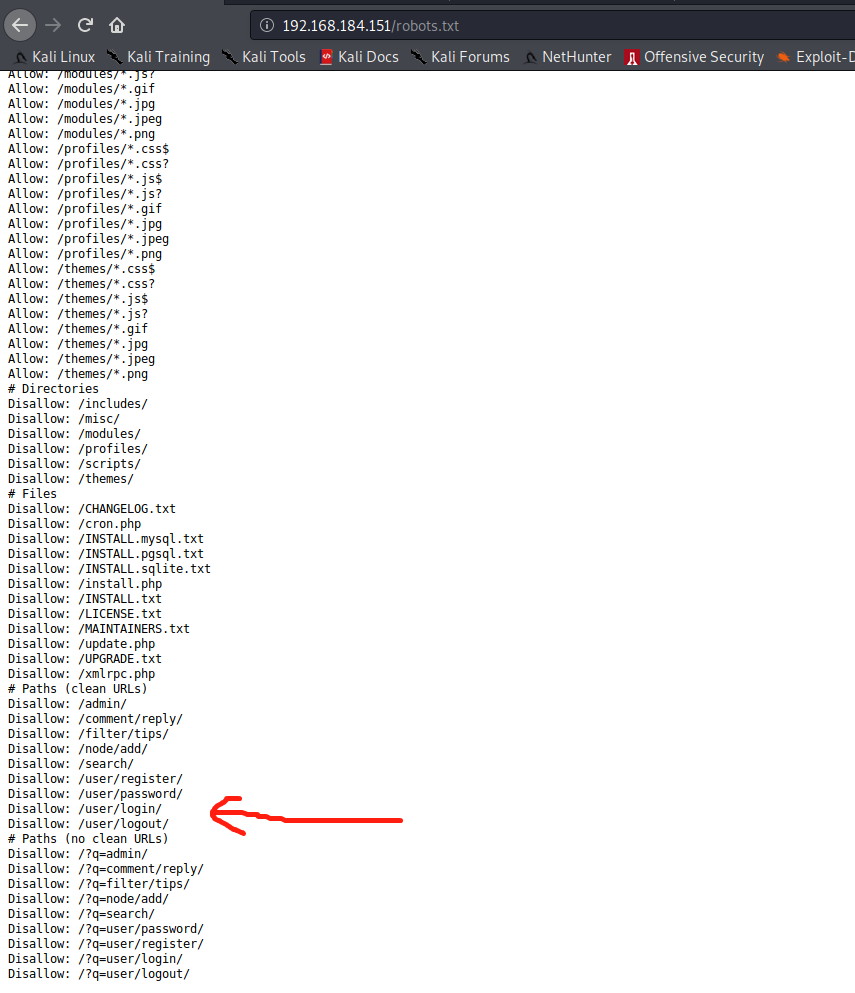


尝试过用在线解密卒，只能用万能的John了，只能跑出一个用户名密码

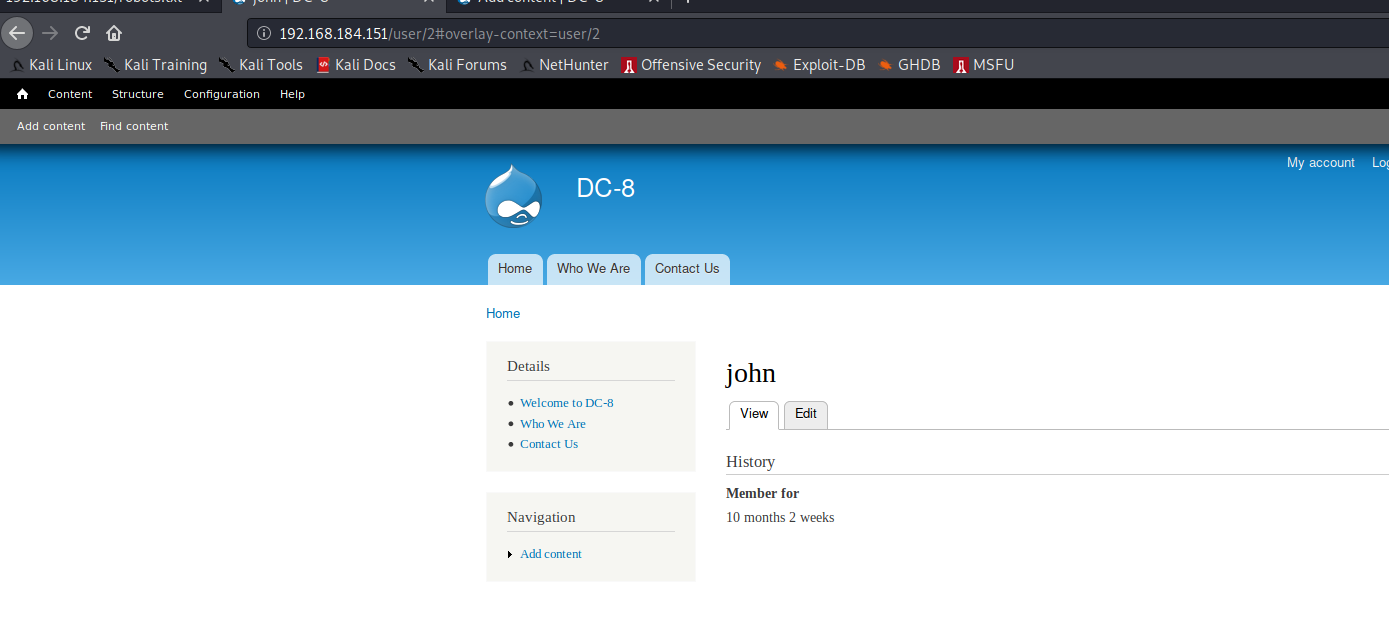
John turtle



这里我尝试输入常见的路径名/robots可以正常回显而且发现有个/login的地方

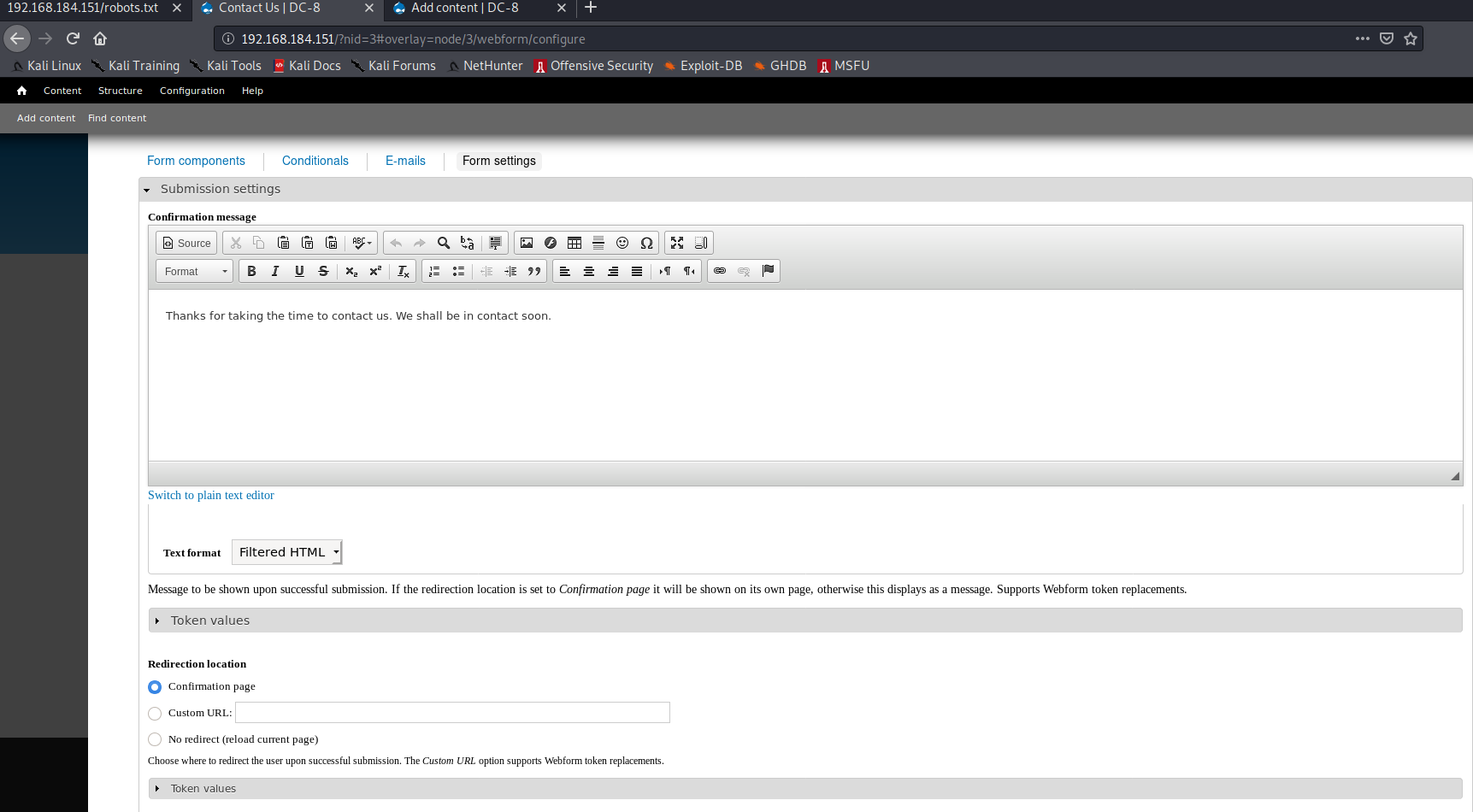


输入完john的账号密码信息以后成功登录

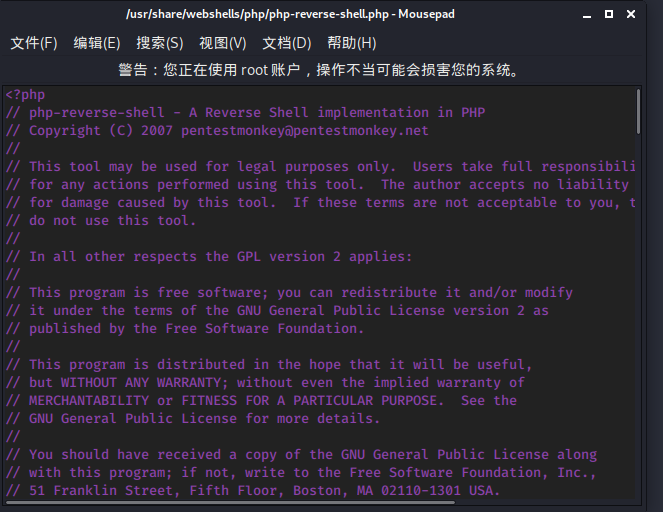


# 0x03:上传反弹shell

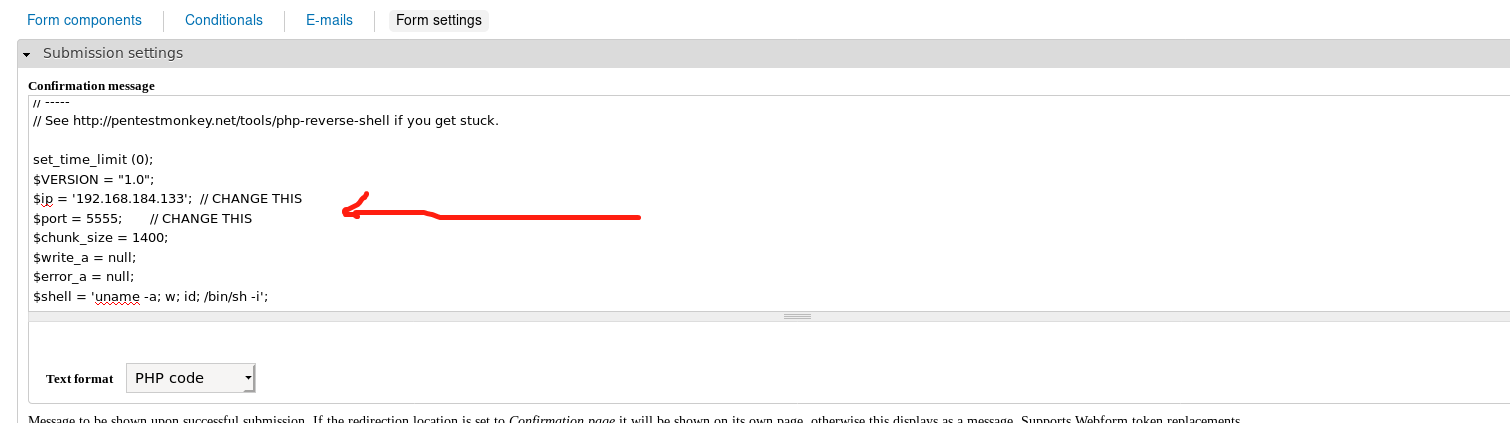
登录以后来到contact us这里似乎可以调text format变成php格式



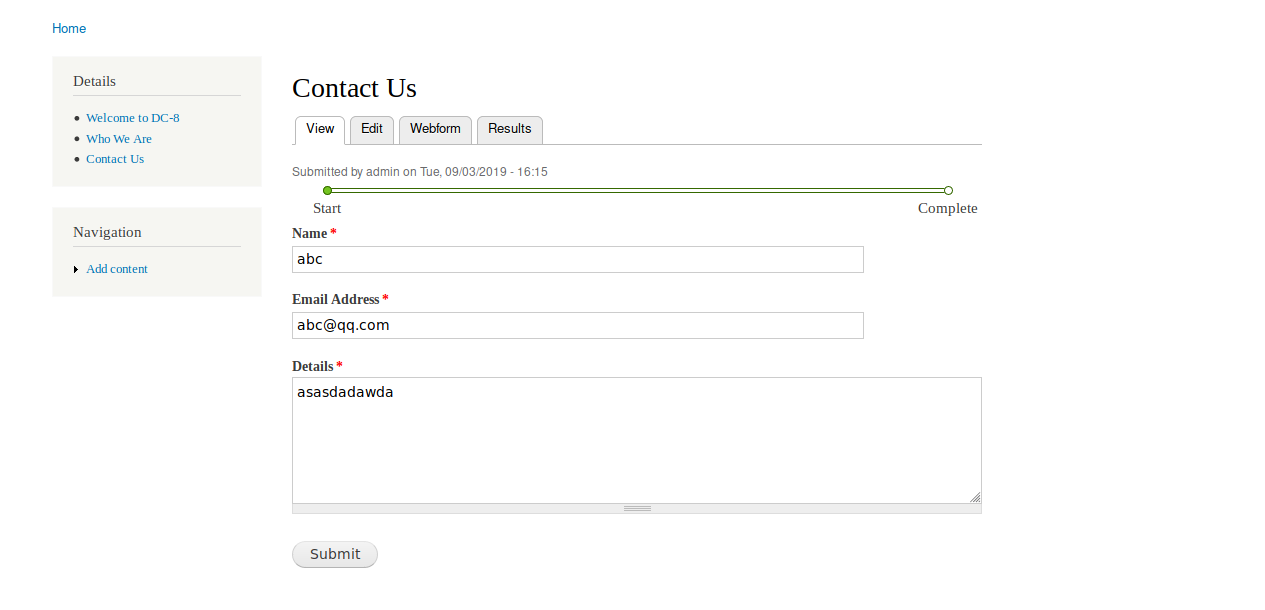
先到/usr/share/webshells/php/php-reverse-shell.php把里面的代码复制下来



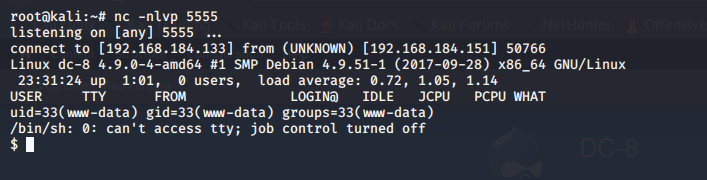
放上去，记得把ip改为kali IP可以不用改端口一定要把text format调成php模式



然后在contact随便输入点东西提交

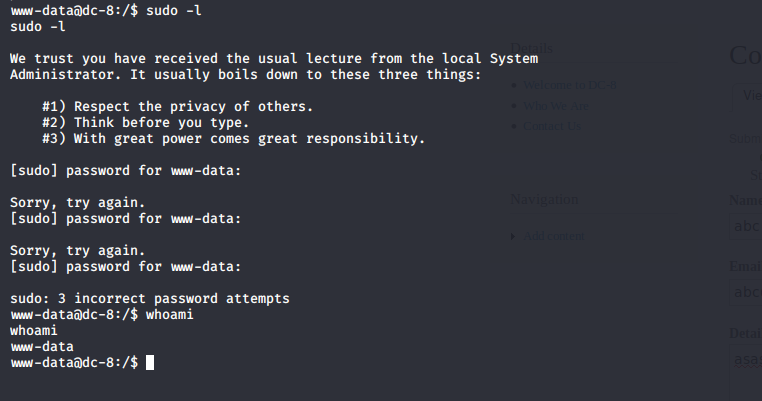


记得提前开启netcat，成功反弹

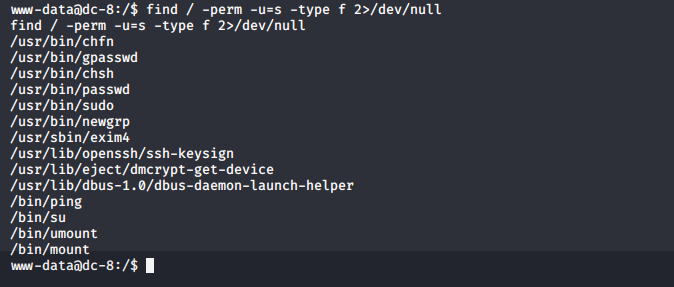


# 0x04:提权

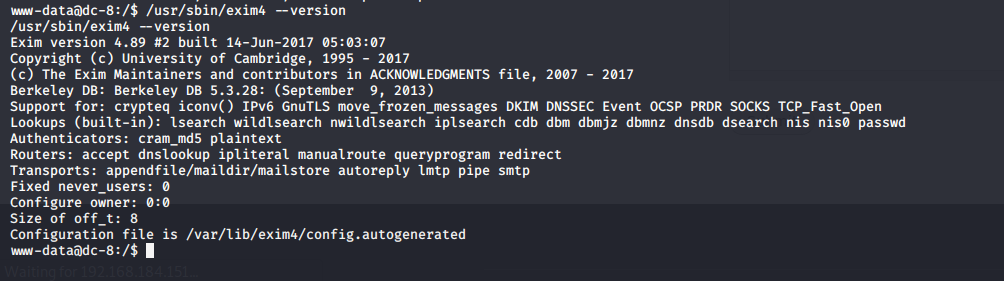
这里首先尝试用sudo -l然而不知道密码卒



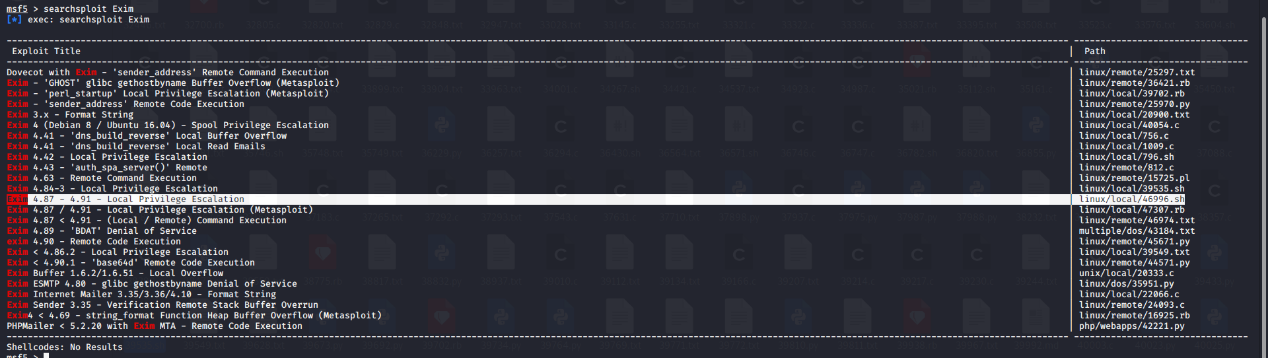
换个思路­找找哪些文件有SUID权限发现一个特别的东西exim4,exim4是一个邮件传输代理服务器软件，曾经曝出过严重漏洞



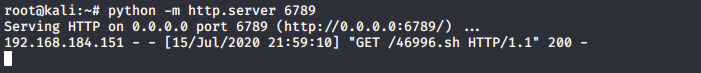
--version查看到版本为4.89



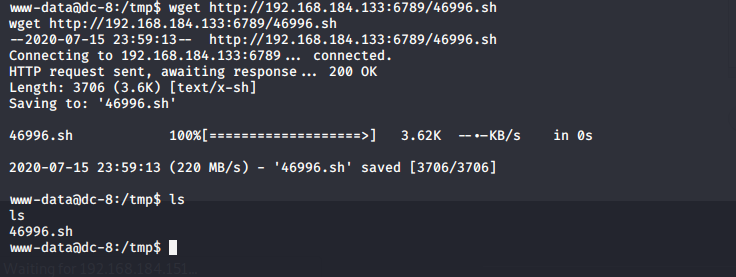
用MSF搜索一下发现一个符合版本的本地提权



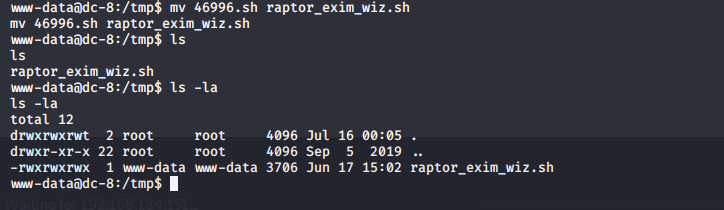
先把该脚本复制到/root目录下好操作，然后利用python开启共享模式



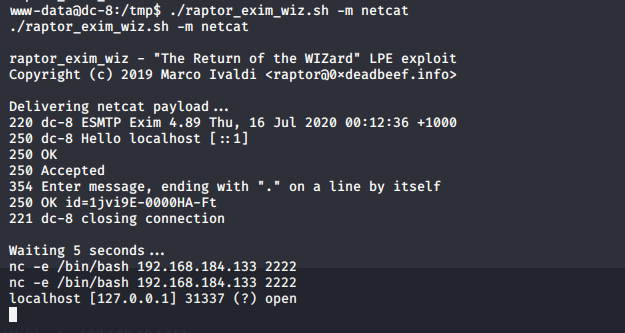
再用wget把它传上去



这里看了一下使用方法我觉得先把它改个名方便执行



查看了下脚本运行方法为名字 -m netcat,然后在塞一条反弹shell进去一定要快



最后得到权限可以读到flag

