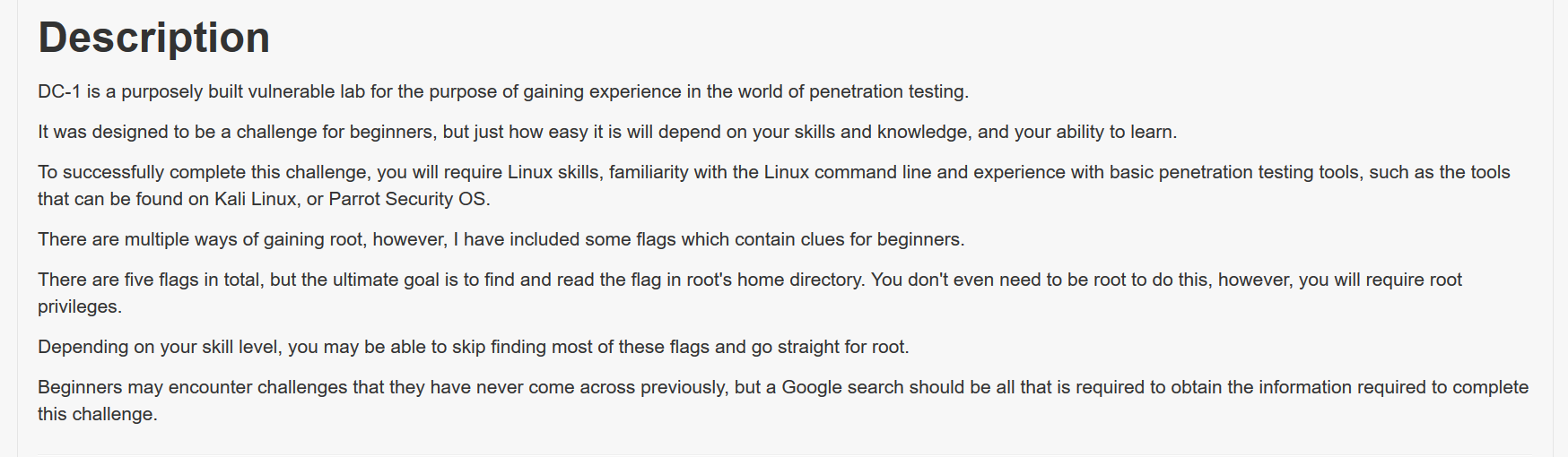
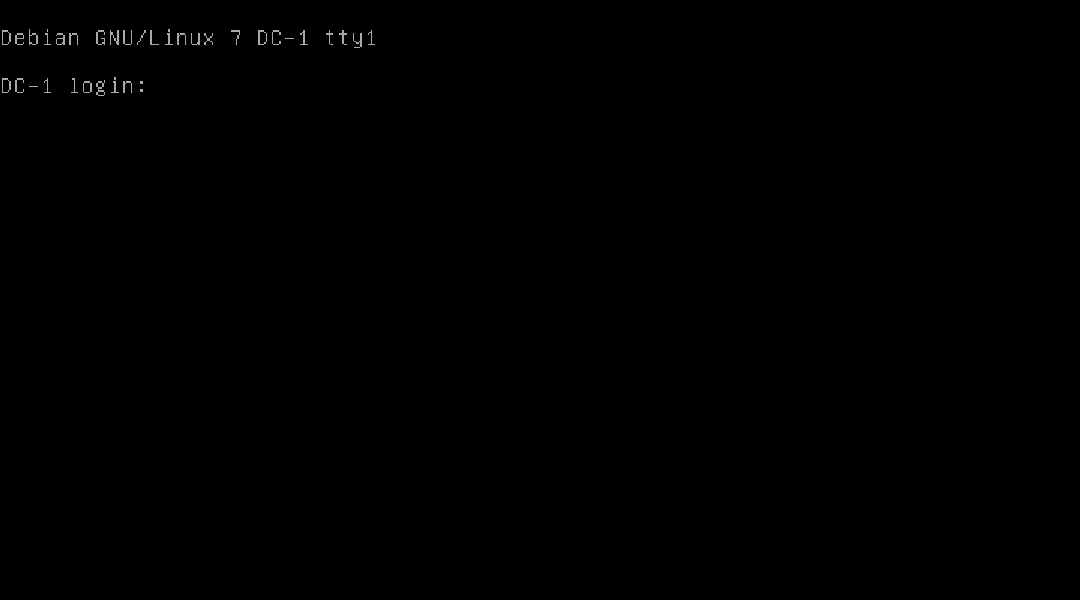
# 0x00:下载链接

下载链接: <https://www.vulnhub.com/entry/dc-1-1,292/>

总的来说就是新手级别，总共有5个flag建议在VirtualBox下运行



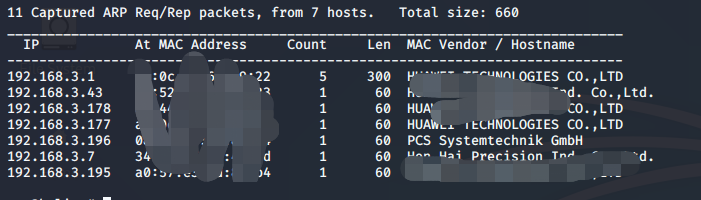
不过VirtualBox确实方便，解压以后导入运行即可，默认桥接网卡模式就行了



# 0x01:探测靶机

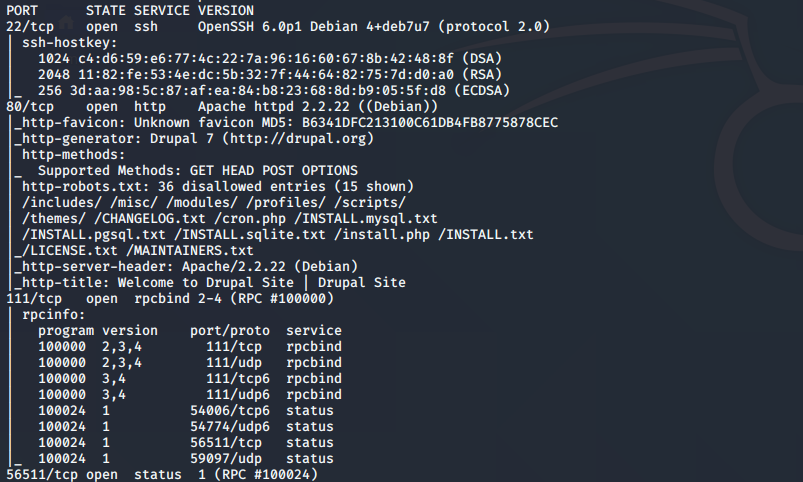
先用netdiscover探测一下靶机IP,由于有之前的经验直接找PCS，可以确认靶机IP为192.168.3.196

命令:netdiscover -r 192.168.3.0/16

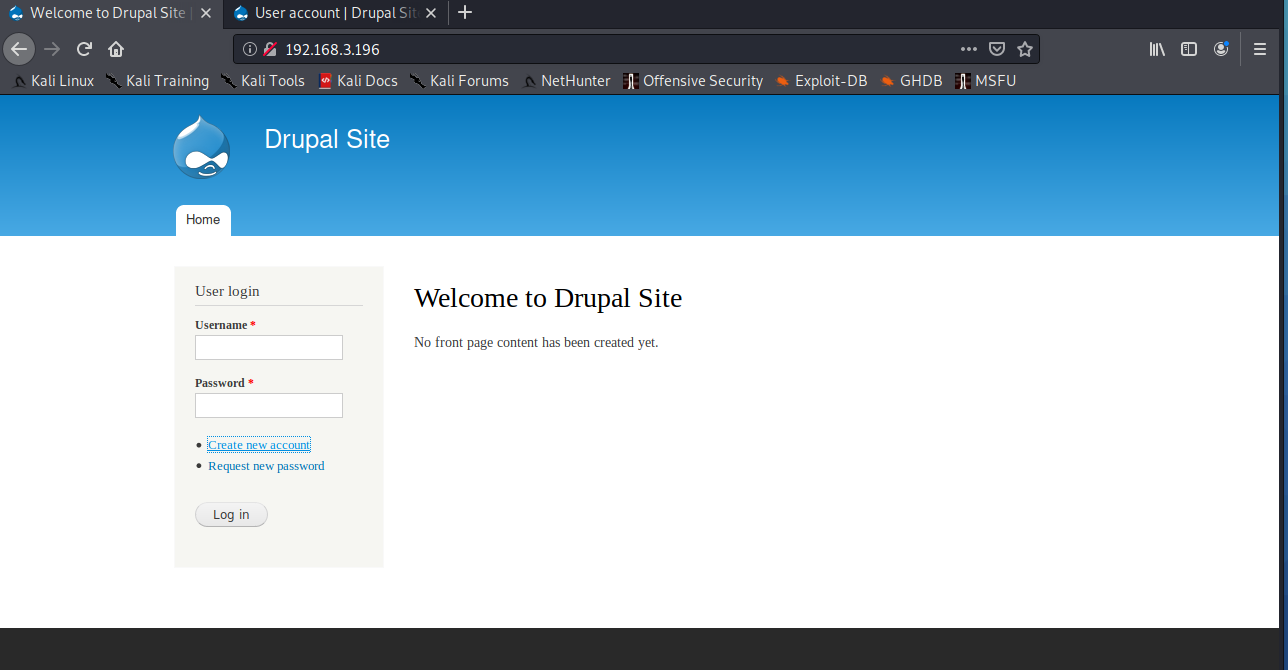


然后开始用nmap探测波端口，主要开了22，80，111和56511端口

命令:nmap -A -sS -sV -v -p- 192.168.3.196

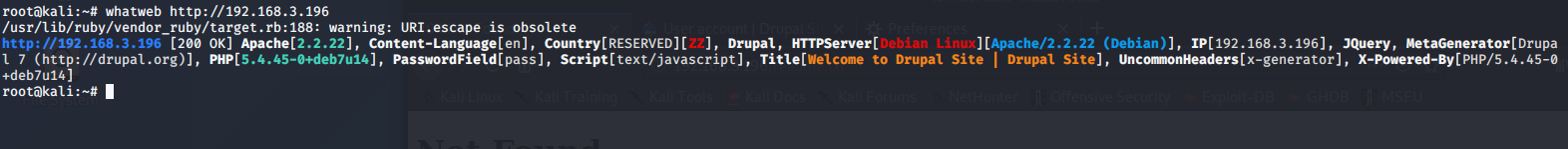


先正常访问一下IP可以正常回显

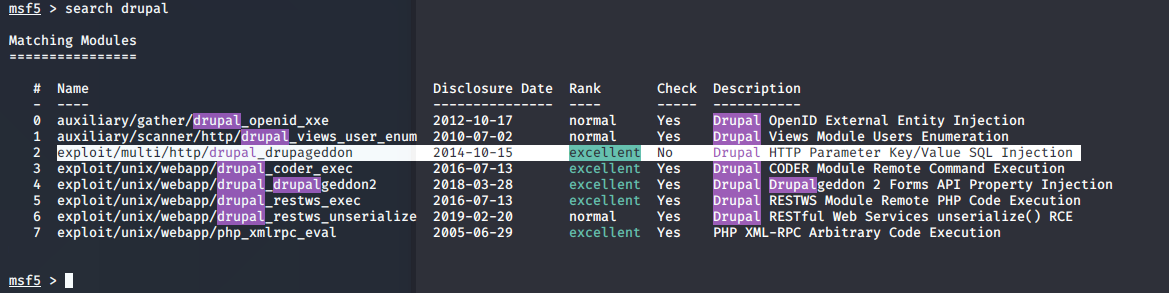


# 0x02:挖掘漏洞

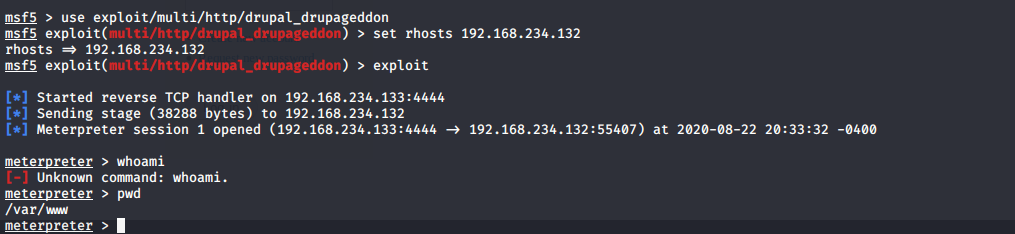
由于首页有个很大的水滴头很像个CMS用whatweb查了下是Drupal CMS版本为7



由于页面功能比较少尝试用Burp抓包登录数据用SQLMAP跑结果跑不出来，只能用MSF搜索一下，找到一个SQL注入的payload

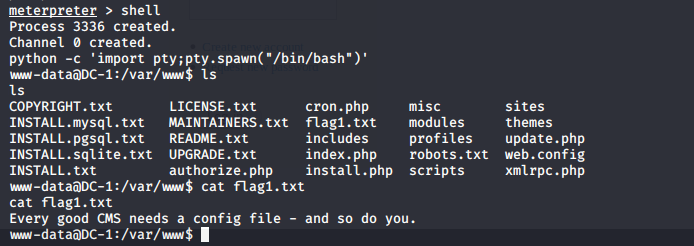


这里用第二个payload，参数比较简单只需要设置rhost(ip就行了，这里我的virutalbox上的kali的MSF有点笨比，死活运行不了，只能搬回VM重新分配IP，幸好还可以运行)出现了meterpreter就是代表成功了

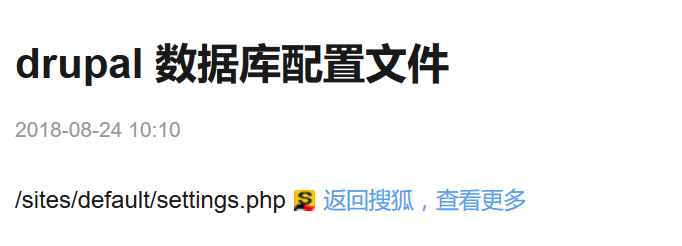


# 0x03:挖掘第二个flag

先进入shell模式然后输入一个python交互式shell好看一点然后ls成功得到第一个flag，提示是关于CMS的配置文件

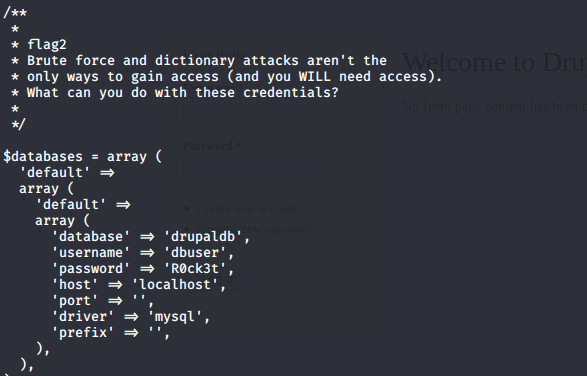


上网查了一下是在这里



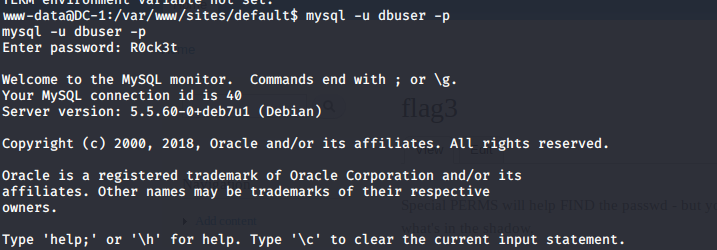
Cat /sites/default/settings.php以后得到flag2的提示是可以进行爆破emmm这里猜测可能是用户的意思，不过不是网站用户而是这台服务器上的用户，因为我们都getshell了。

顺便得到一个数据库的账号密码 dbuser R0ck3t

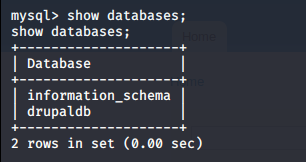


# 0x03:挖掘第三个flag

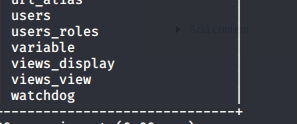
由于有一个数据库账号密码所以输入刚才得到的数据库信息成功进入mysql



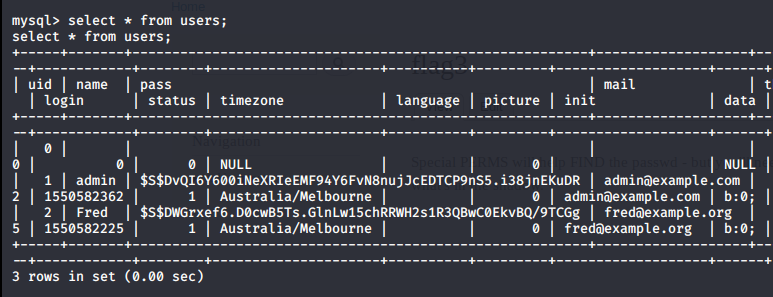
查看表，果断选择drupaldb



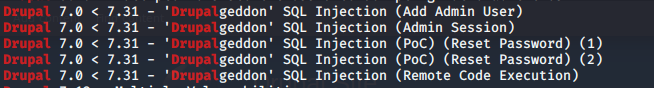
跟进一下发现一个user表



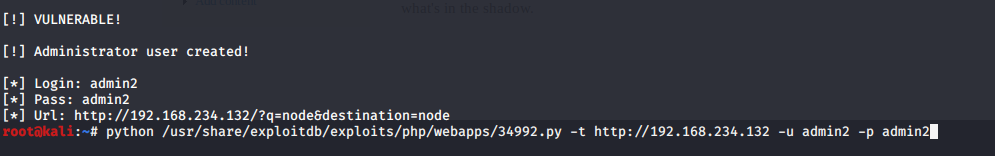
查看里面的内容得到admin账号，然而emmm这是这个CMS特有的加密方式普通MD5解密不了



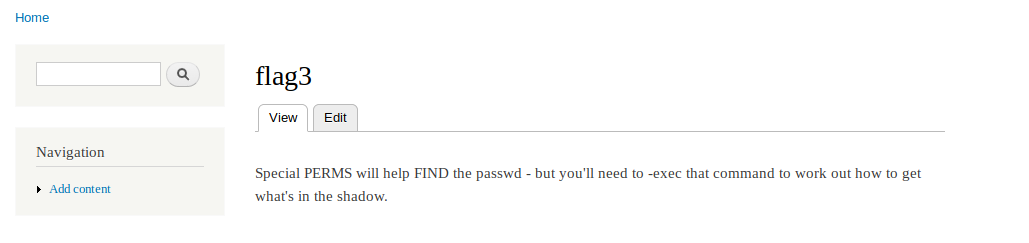
返回MSF的时候用searchsploit发现一个添加管理员的py文件



看了一下用法比较简单只要指定域名，然后输入账号密码就行了

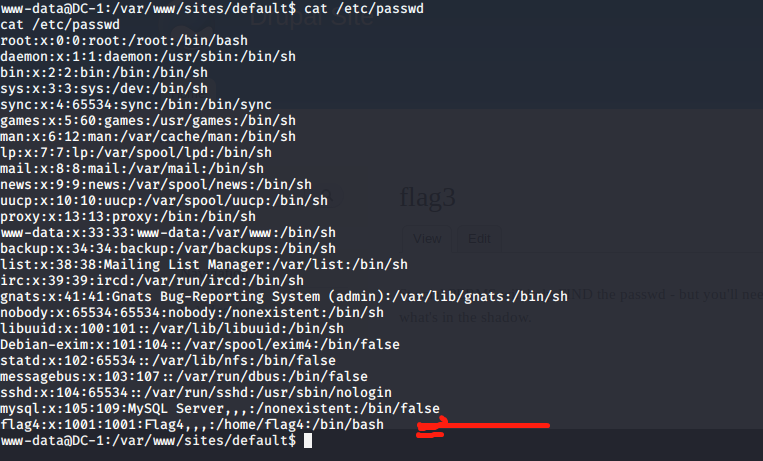


成功登录以后看到flag3顺便得到提示

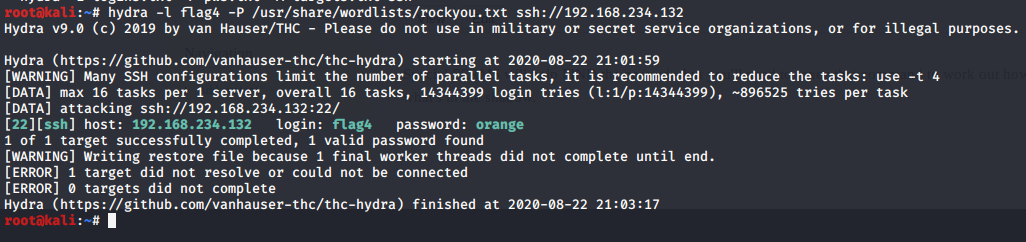


# 0x04:挖掘第四个flag

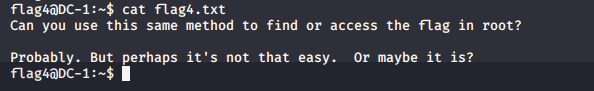
原本想用cat /etc/shadows的但是没得权限，只能用 cat /etc/passwd发现一个flag4的时候结合刚才的提示应该是要爆破的



那爆破ssh一般是用hydra，字典的话就是/usr/share/wordlists/rockyou.txt或者是John自带的密码字典也可以的

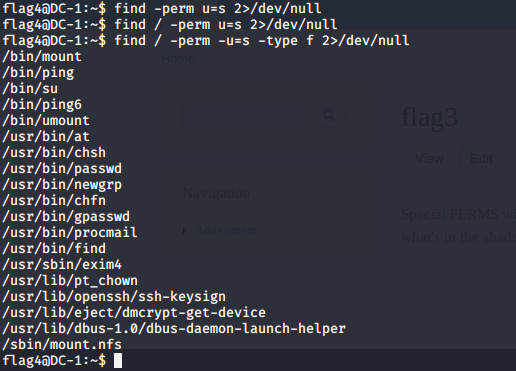


登录以后得到第四个flag



# 0x05:提权

最后一个flag应该就是在root目录下了，用了sudo -l还是一如既往的挂掉，换成find / -perm -u=s -type f 2>/dev/null，看到find



关于find提权的话可以继续这篇文章<https://www.cnblogs.com/nul1/p/11309287.html>，先创建一个文件然后就用find 文件在后面加入你想要的命令，最后直接读取flag

