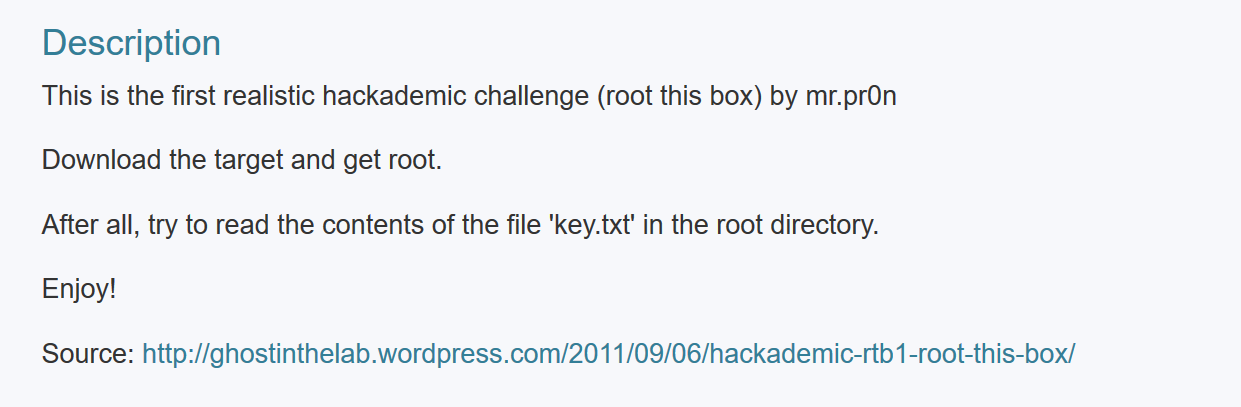
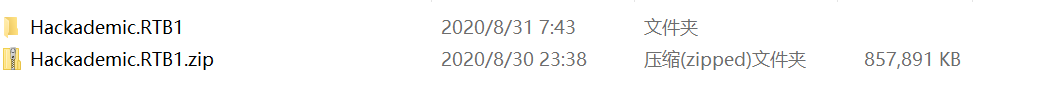
# 0x00:下载链接

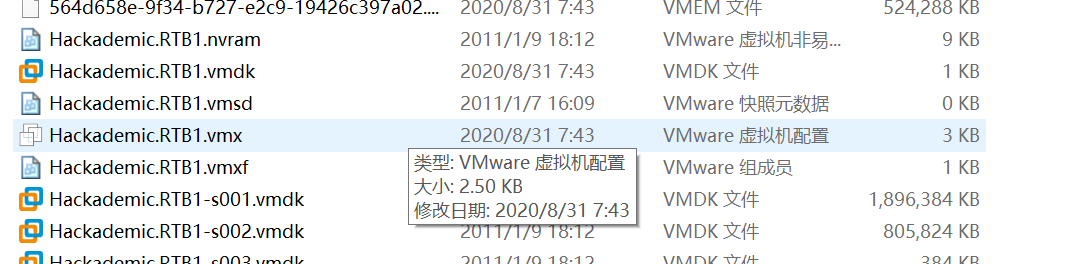
下载链接: https://www.vulnhub.com/entry/hackademic-rtb1,17/



下载好以后有解压有个文件夹点进去



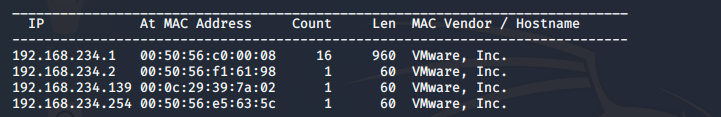
然后点击.vmx就行了由于会默认跳到NAT所以直接运行就可以了



# 0x01:探测靶机

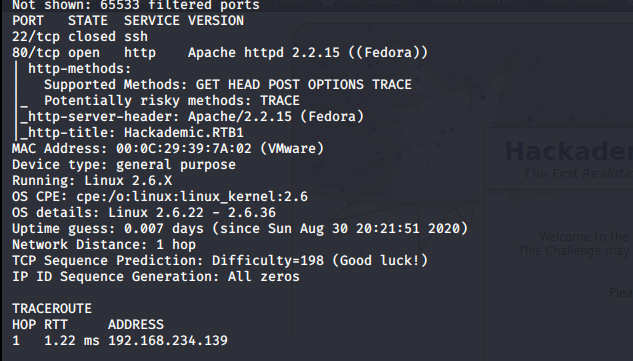
先用netdiscover确认靶机IP，排除.1,.2和.254可以确认靶机IP为192.168.234.139

命令:netdiscover -r 192.168.234.0/16

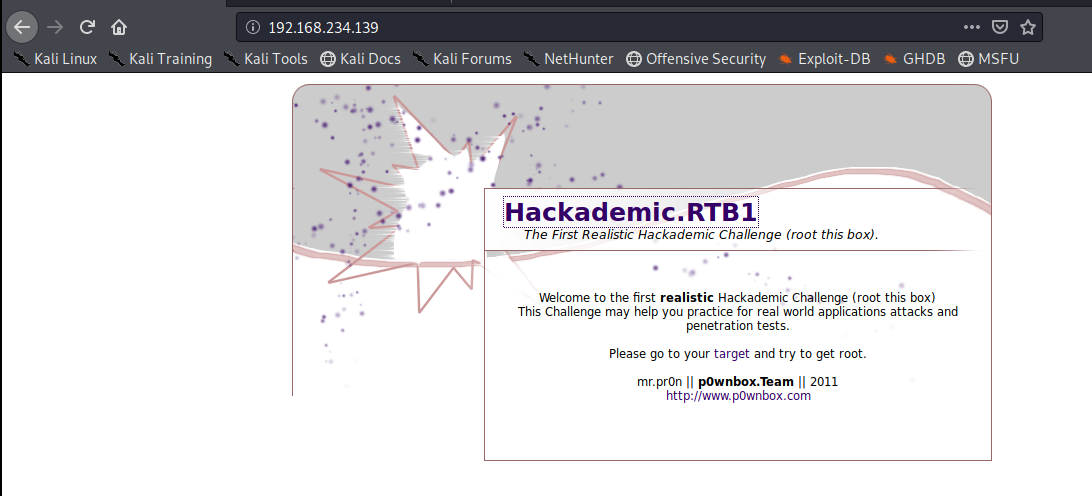


然后用nmap探测一波端口这次开放的端口比较少，只有22和80

命令:nmap -A -sS -sV -v -p- 192.168.234.139

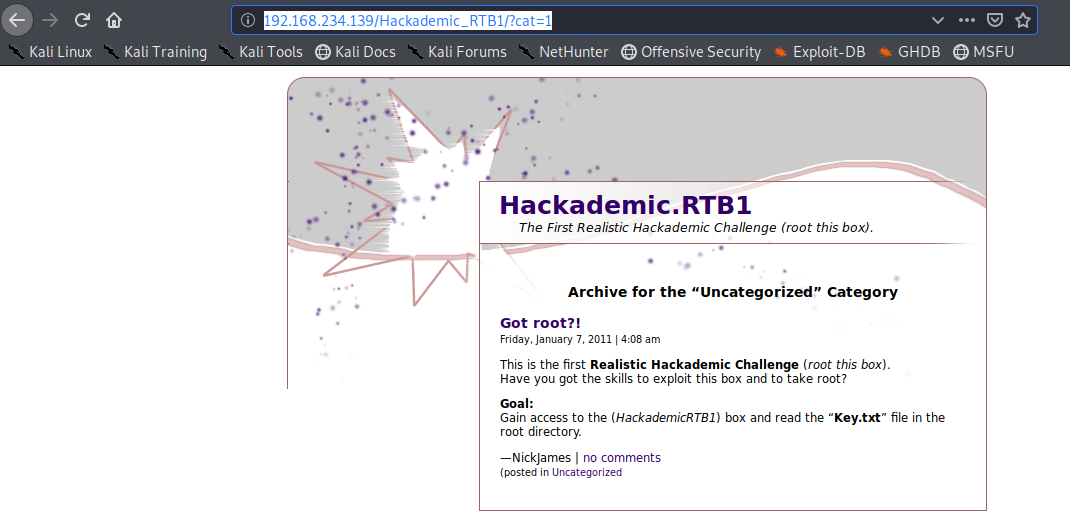


访问一下IP可以正常访问开搞



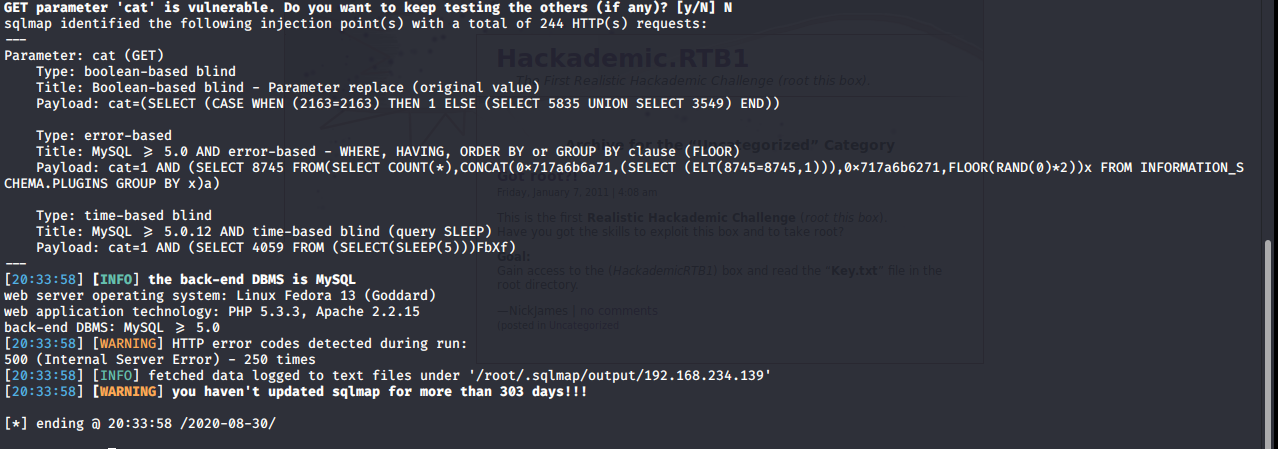
# 0x02:漏洞挖掘

点击了一下下面的post in Unauthorized弹出一个xxxx?cat=1的网址



放到sqlmap里面启动直接跑出来

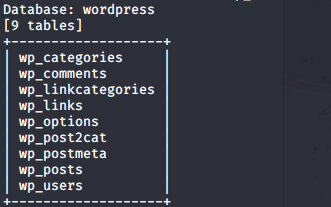
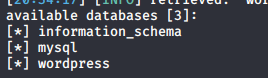
命令:Sqlmap -u 网址



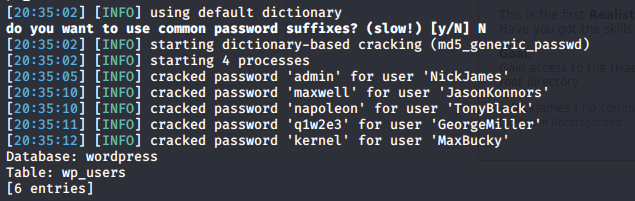
然后继续跟进发现一个名为wordpress的数据库，查看里面发现一个wp\_users的表

命令:sqlmap -u 网址 --dbs

Sqlmap -u 网址 –dbs -D wordpress --tables

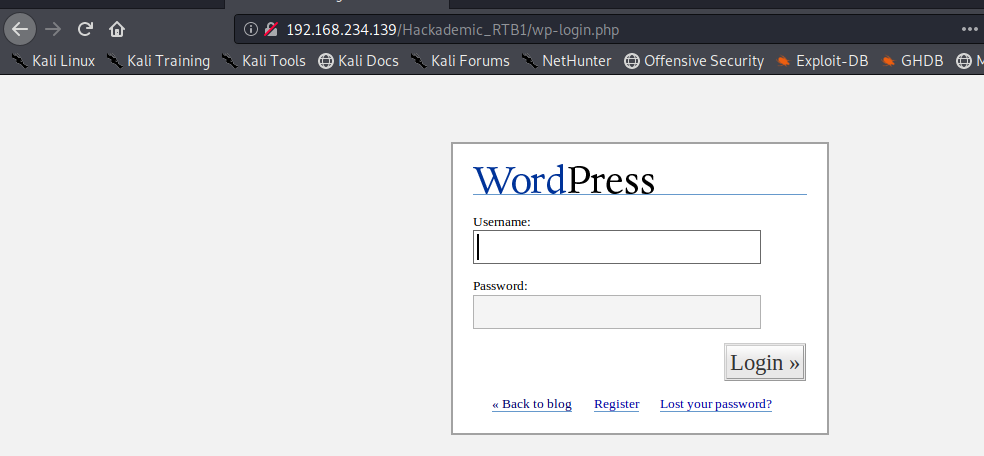


然后跑里面的内容可以直接解密得到几个用户名和密码

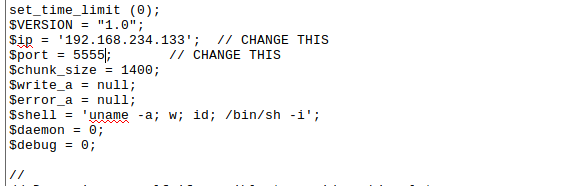


# 0x03:上传反弹shell

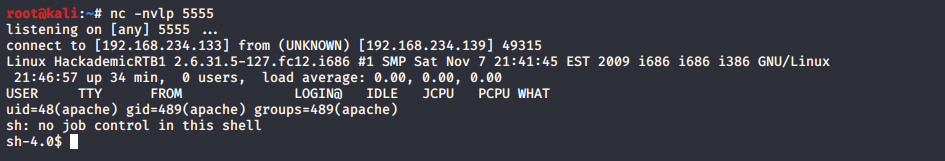
输入默认的登录路径可以正常回显。。。。应该庆幸wordpress的默认登录界面从来没改过



找到能上传php文件的地方用kali自带的反弹shell(/usr/share/webshell/php/php-reverse-shell.php)贴上去，记得把ip改为kali的ip然后端口随便设置一个新的

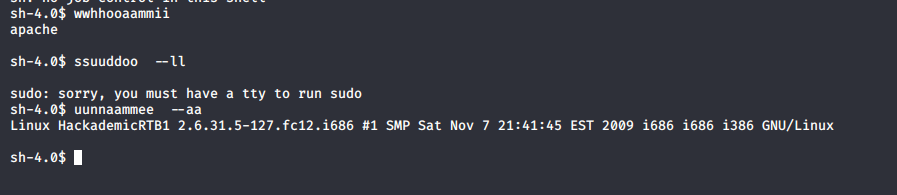


提前开启netcat就可以得到一个shell了

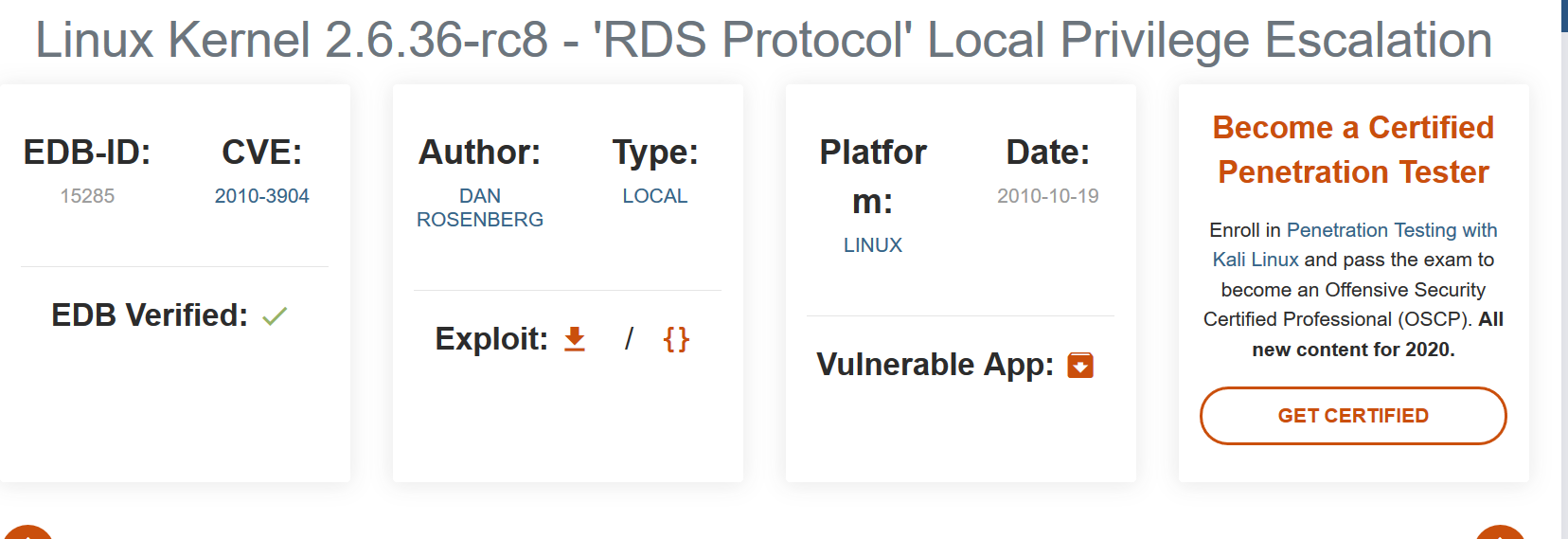


# 0x04:提权

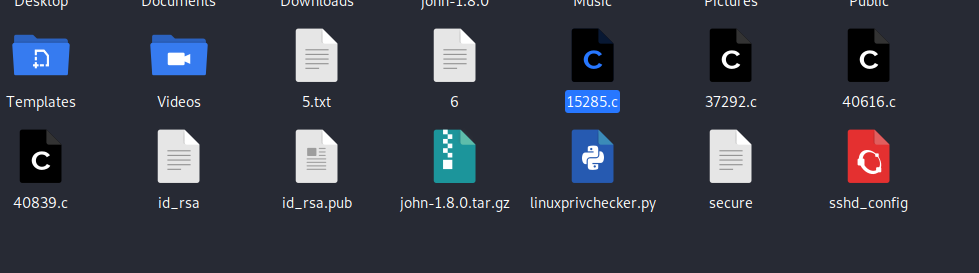
这里出了点bug输入的内容会双写，不要在意细节。首先输入sudo -l回显不了卒，查看到版本号为2.6，低版本的内核有很多payload可以进行提权



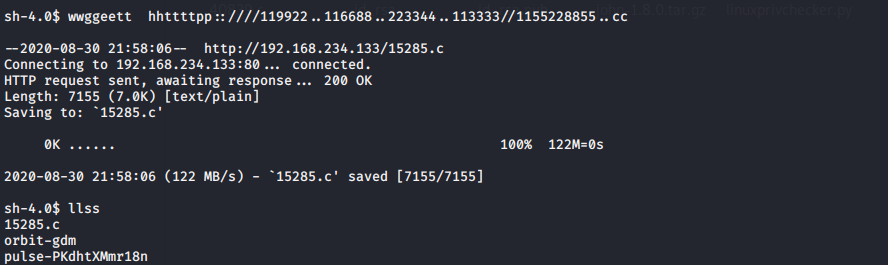
这里在exploitdb搜索到一个payload下载下来



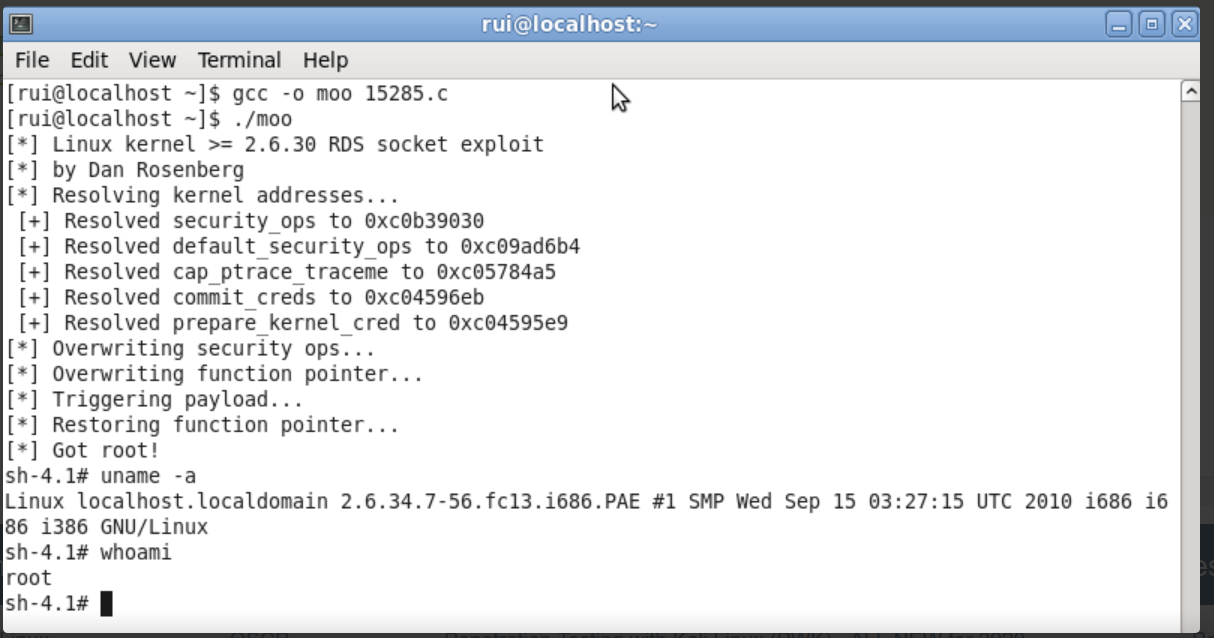
然后复制到kali里面



开启共享模式，然后回到shell那里用wget下载下来不要在跟目录下载建议去到/tmp目录下



关于使用方法在上面那个exploitdb的payload下面有一张图片有使用方法



跟着作者给出的步骤最后成功进入到shell模式成功读取到key（这次终于正常输入了）

