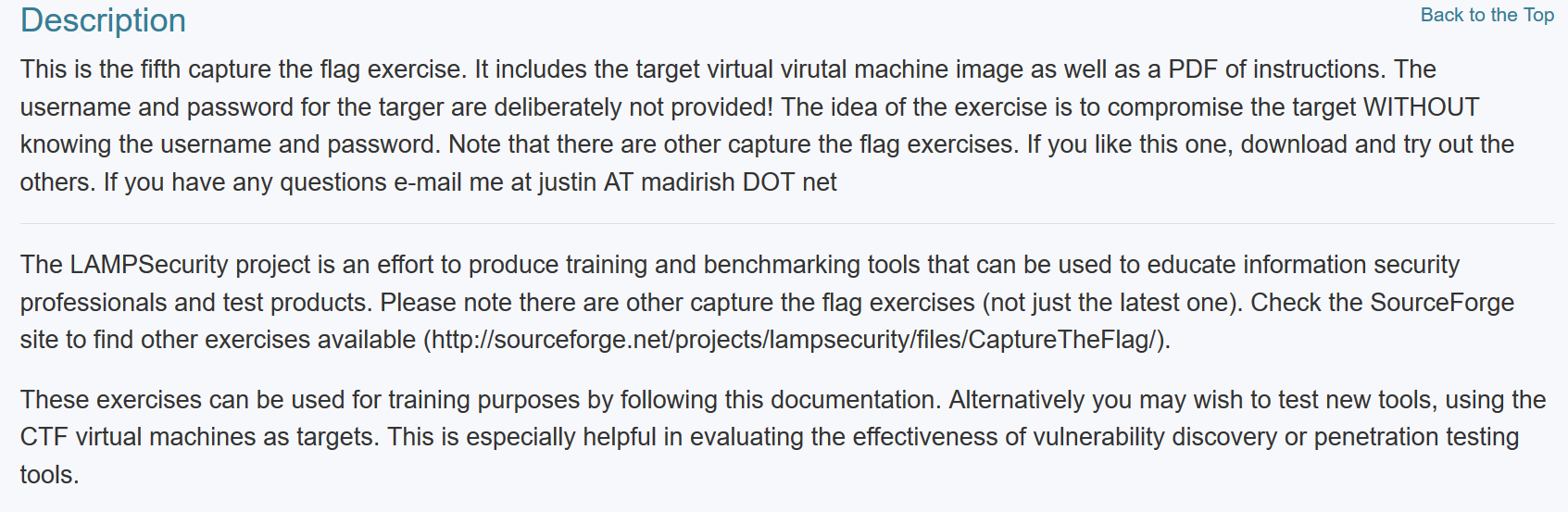
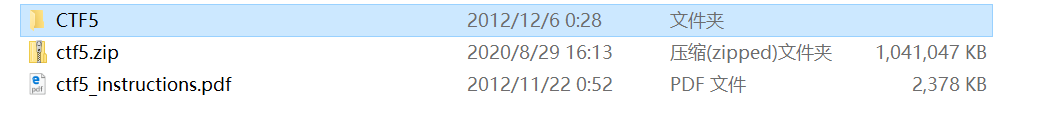
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/lampsecurity-ctf5,84/>

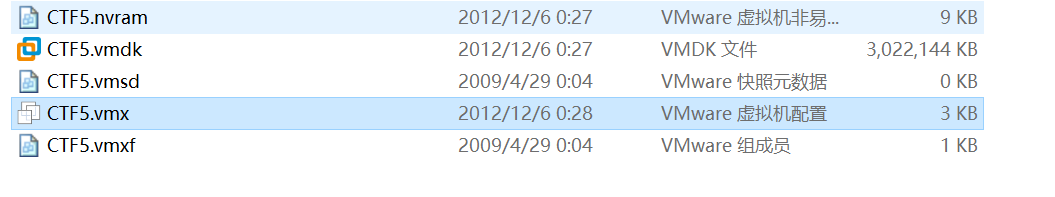
继续做一下这个十一年前的系列，目标还是得到flag



下载完后解压得到两个文件点击CTF5



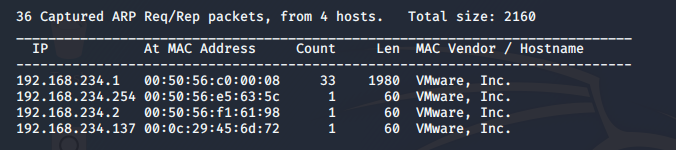
点击其中的.vmx就会在VM下自动安装好了，也会调成NAT模式直接运行就可以了



# 0x01:探测靶机

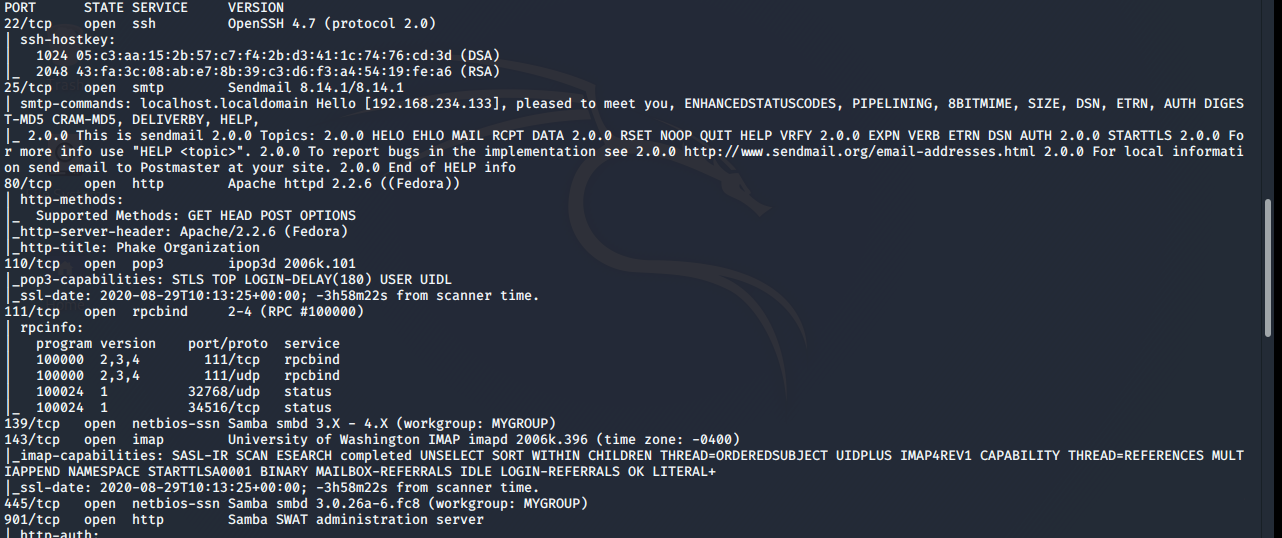
还是先用netdiscover探测靶机IP，排除.1,.2和.137可以确认靶机IP为192.168.234.137

命令:netdiscover -r 192.168.234.0/16

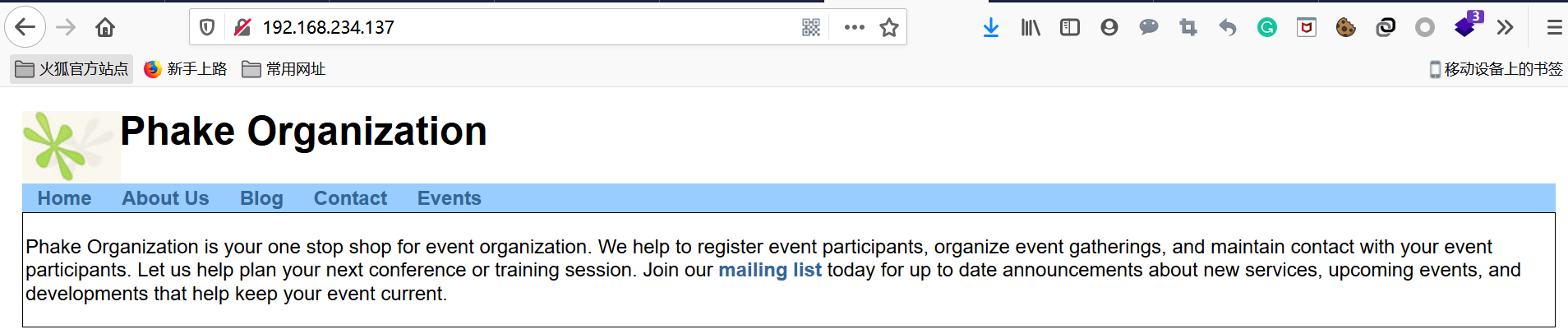


然后用nmap探测波端口这次开放的比较多有22，25，80，110，111，139，143，445，901等端口

命令:nmap -A -sS -sV -v -p- 192.168.234.137

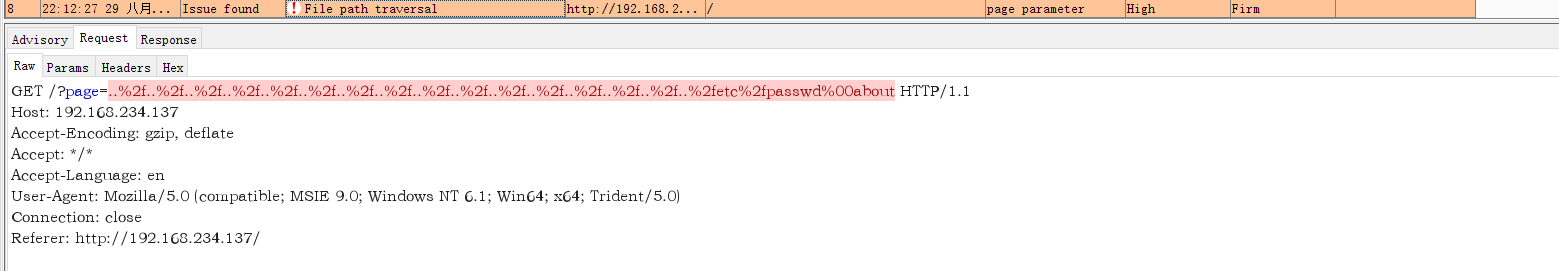


输入一波IP可以正常回显可以开始挖掘了

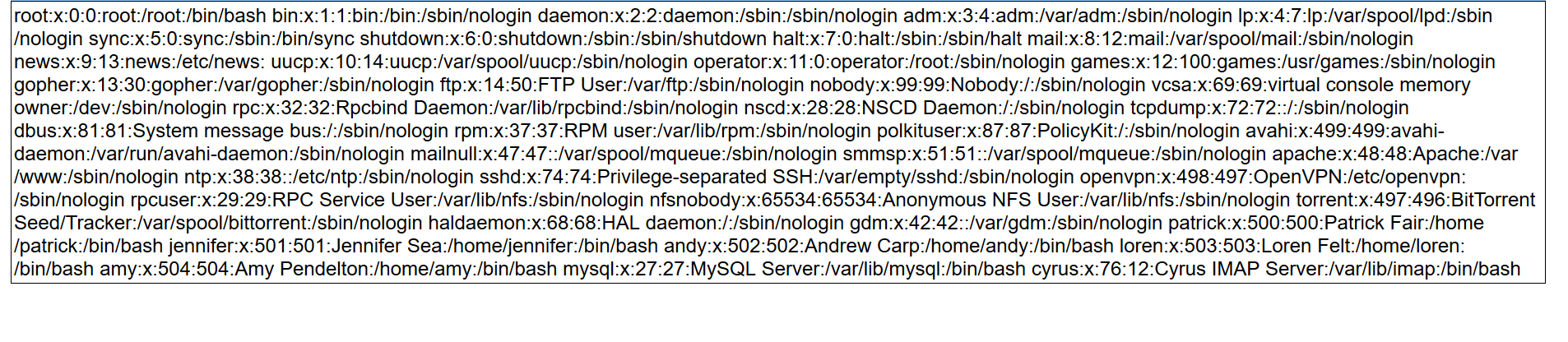


# 0x02:漏洞挖掘

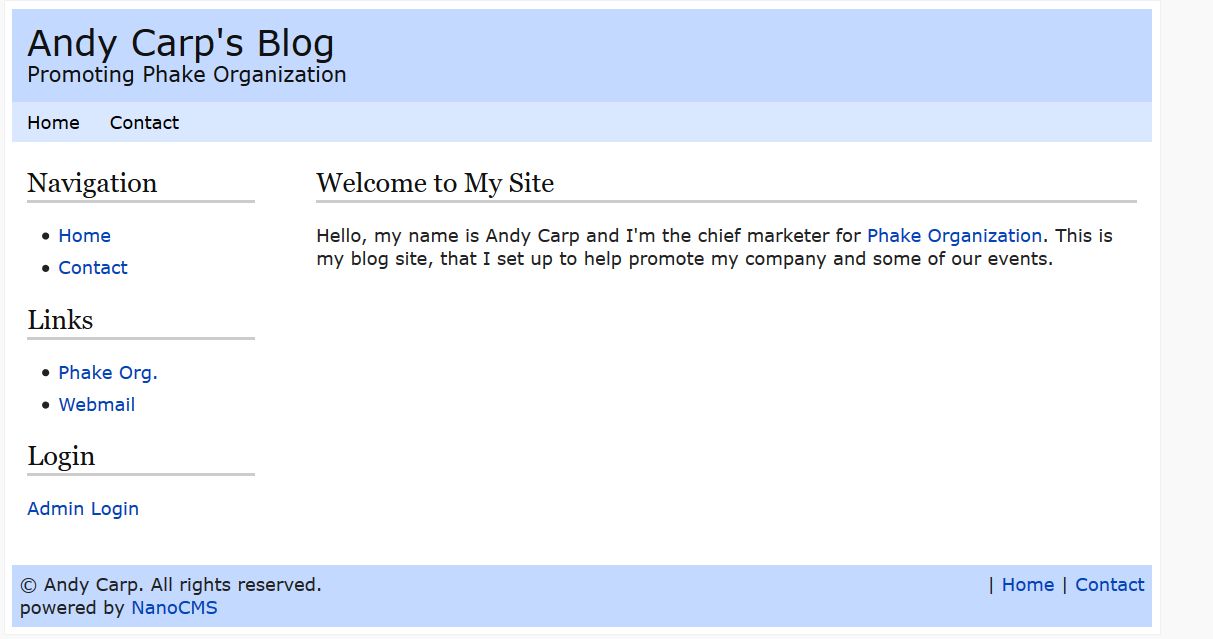
来波降维打击，用Burp的acrive scan扫到一个目录穿越的漏洞



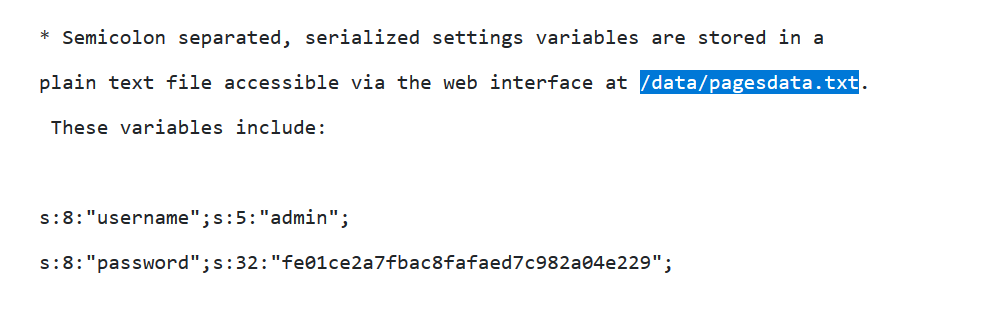
打开验证可以看见一堆账号



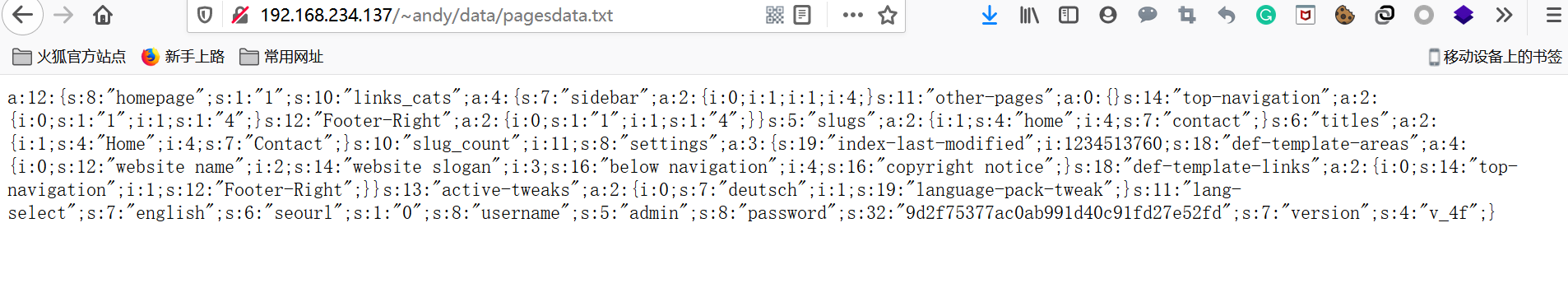
这里在IP首页点击blog会跳转到这个页面。同时注意到左下角有一个NaoCMS



这里搜索了一下<https://www.anquanke.com/vul/id/1052039>有一个前台可以直接读取账号密码的漏洞



直接复制上去看到一堆账号密码，直接看到一个关键词admin

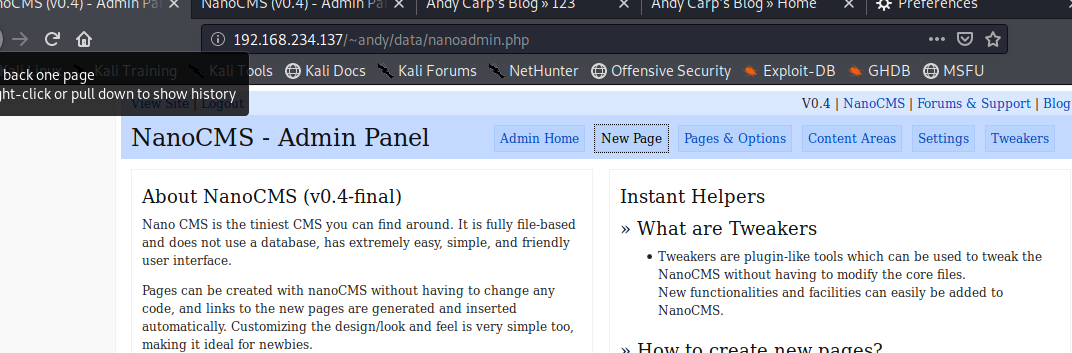


拿去解密可以得到admin的密码

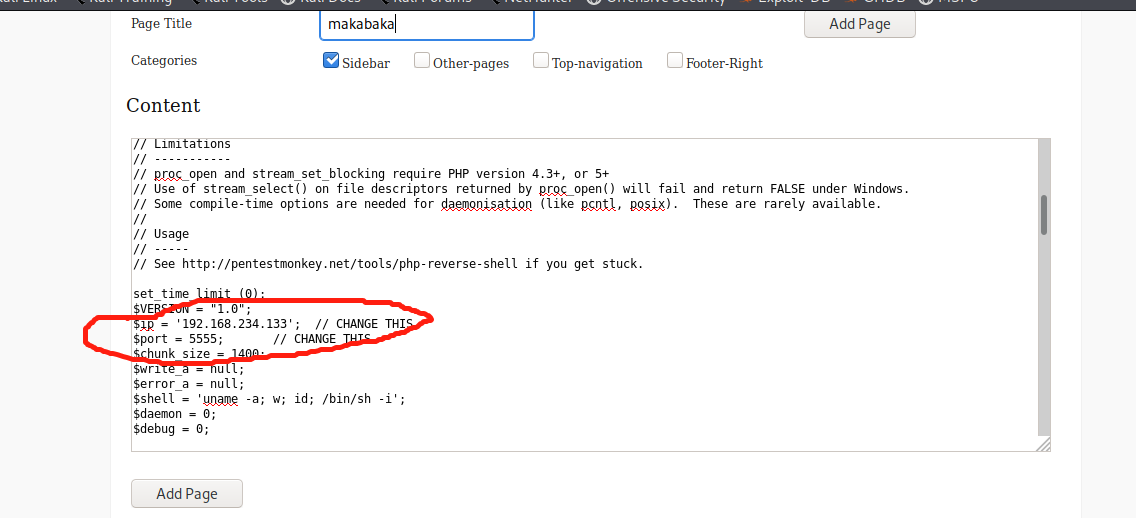


# 0x03:上传反弹shell

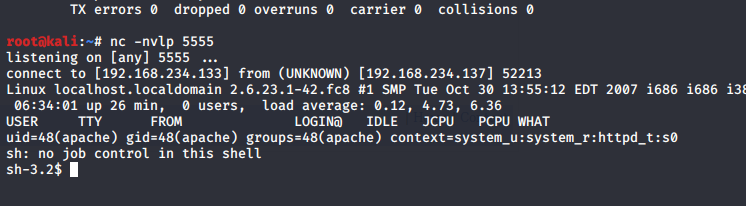
输入刚才得到的admin账号密码以后成功登录，接下来点击new page看看能不能上传反弹shell



关于反弹shell有三种方法，第一种是用MSF能操作，第二种是直接加入netcat一句话，第三种就是用kali自带的反弹shell。这里我用的是kali自带的反弹shell直接复制进去更改成自己的kali ip 和一个端口

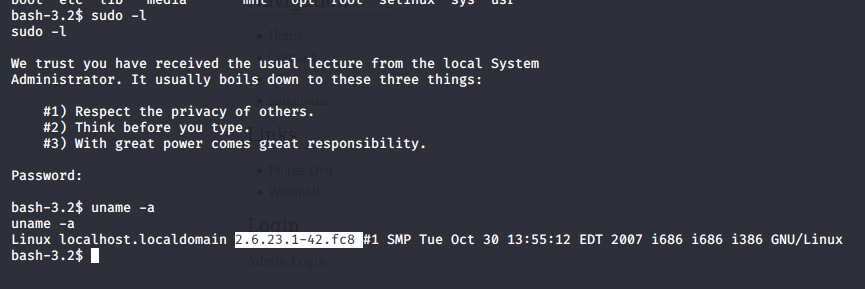


提前用netcat开启你想要的端口，点击Add Page以后在前台点击一下刚新建好的makabaka标签就可以得到反弹shell了

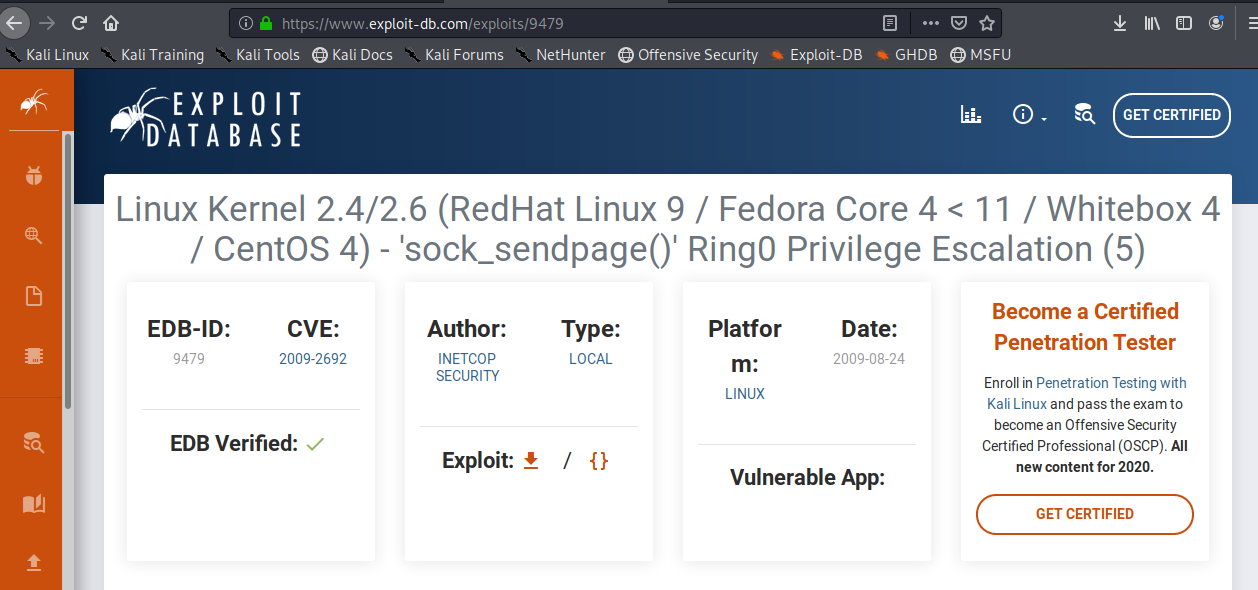


# 0x04:提权

提权其实有多种方法先用uname -a查看一下内核版本号

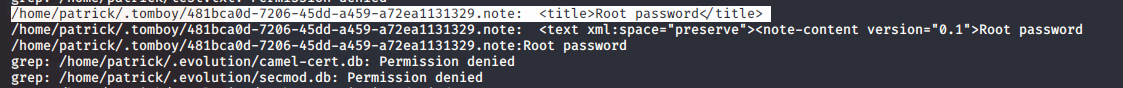


然后去到exploitdb里面找找相关版本的下载然后再传上去提权



也可以用另外一种方法就是直接查找密码，这里找到一个文件内容其标题是root password

命令:grep -R -I password /home/\* (grep是用来搜寻文件或者是匹配内容用的-R是代表会递归指定目录下的所有文件并且匹配其内容在/home目录下的所有文件这里的内容指的是password,然后-i是代表忽略大小写)



跟进一下可以直接看到密码为50$cent直接切换用户得到root权限，然而那时候还没设计好flag

