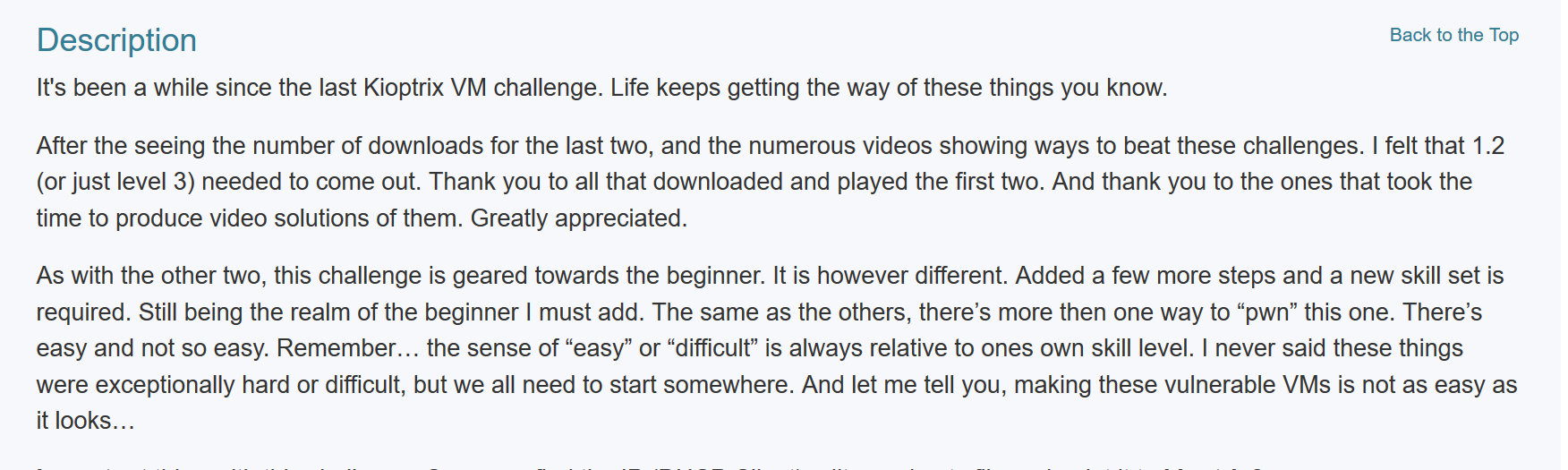
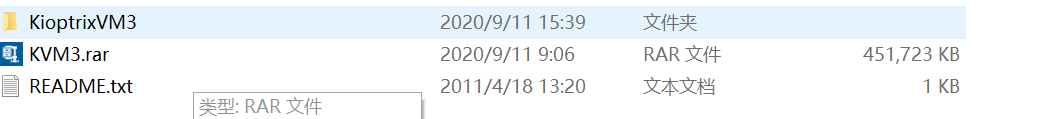
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/kioptrix-level-12-3,24/>

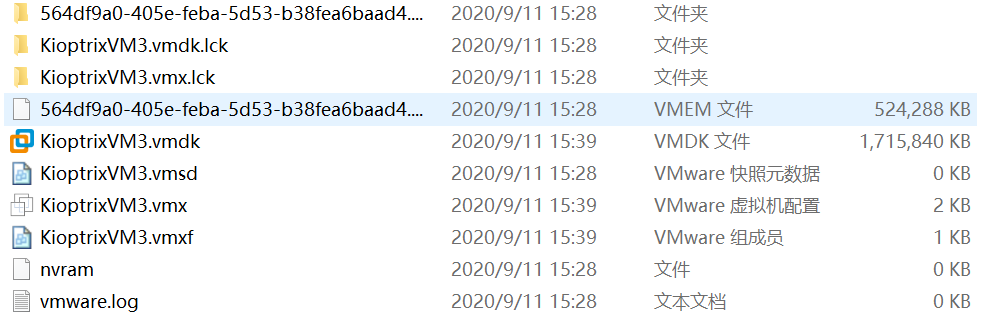
新手靶机但是需要更多的步骤去完成行吧



下载完解压有个文件夹

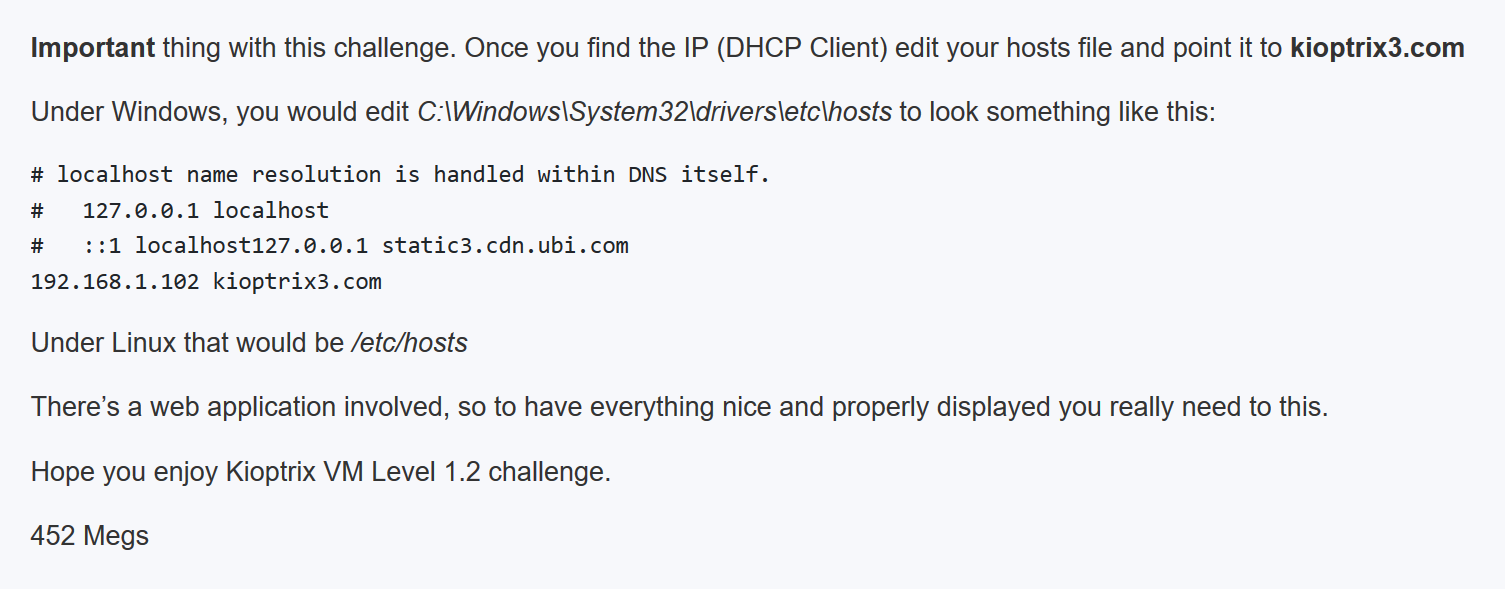


跟进直接点击.vmx顺便调回NAT模式就可以了



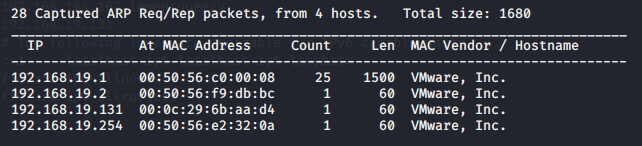
# 0x01:探测靶机

由于在介绍界面建议我们改改host文件所以改一波

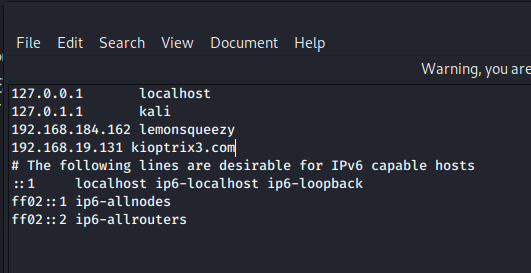


那么先用netdiscover扫一波IP先，排除.1,.2可以确认靶机IP为192.168.19.131

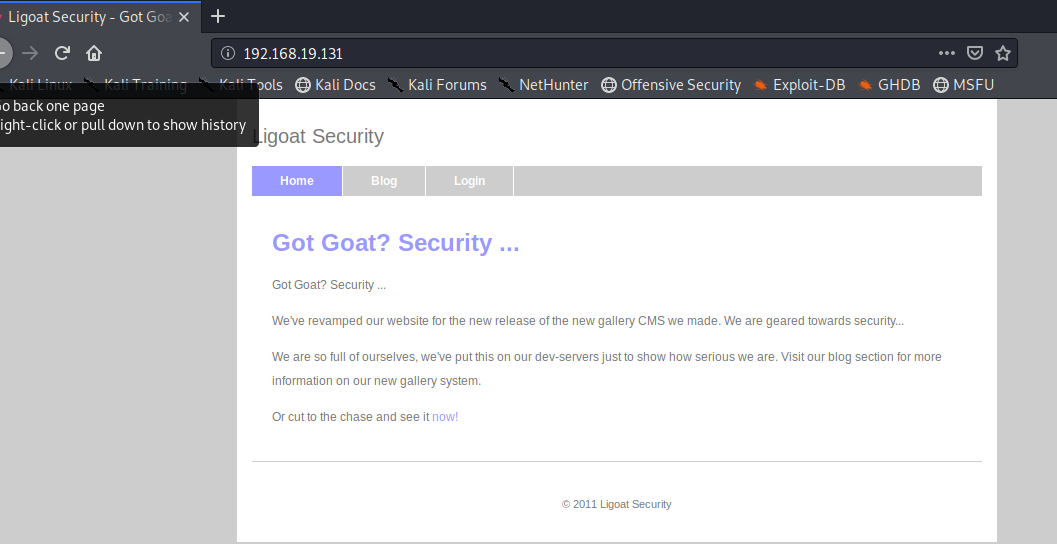
命令:netdiscover -r 192.168.19.0/16



然后打开/etc/hosts(可以用kali自带的Mousepad或者是vim也可以)然后添加靶机IP和名字进去

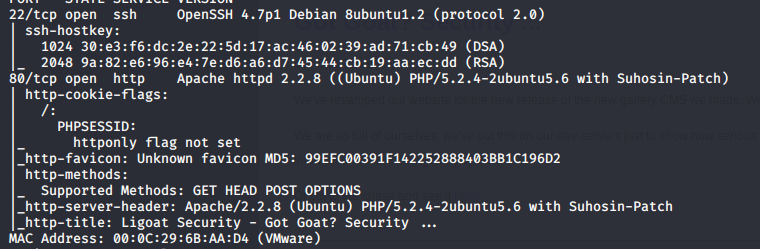


可以正常访问



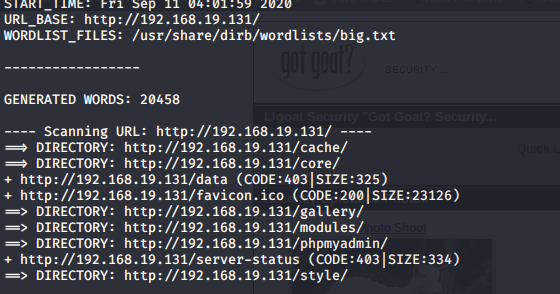
然后用nmap扫波端口只开了22和80

命令:nmap -A -sS -sV -v -p- 192.168.19.131

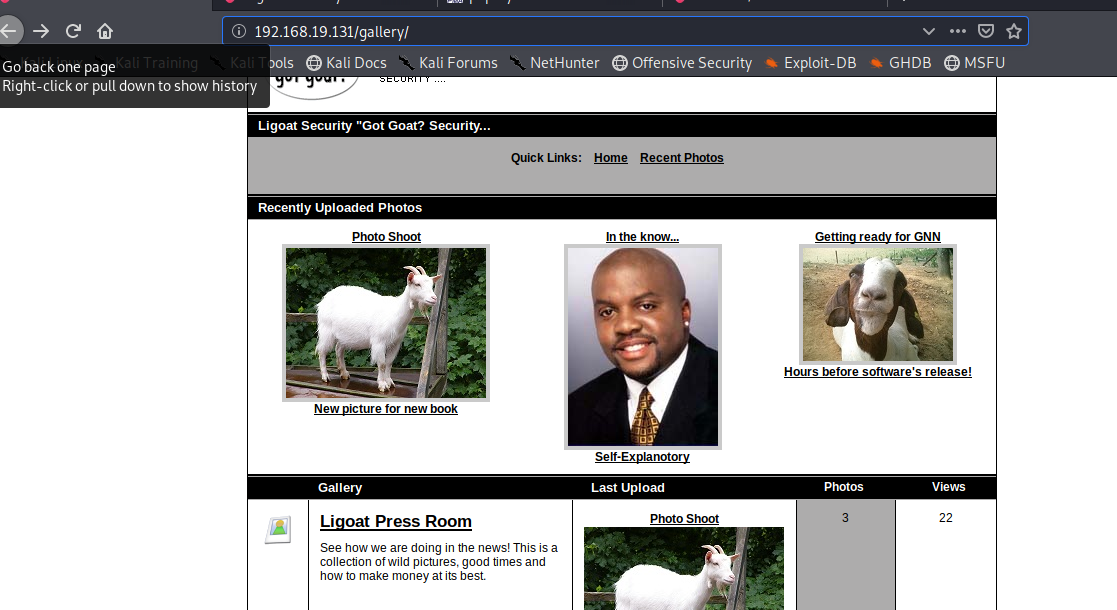


# 0x02:挖掘漏洞

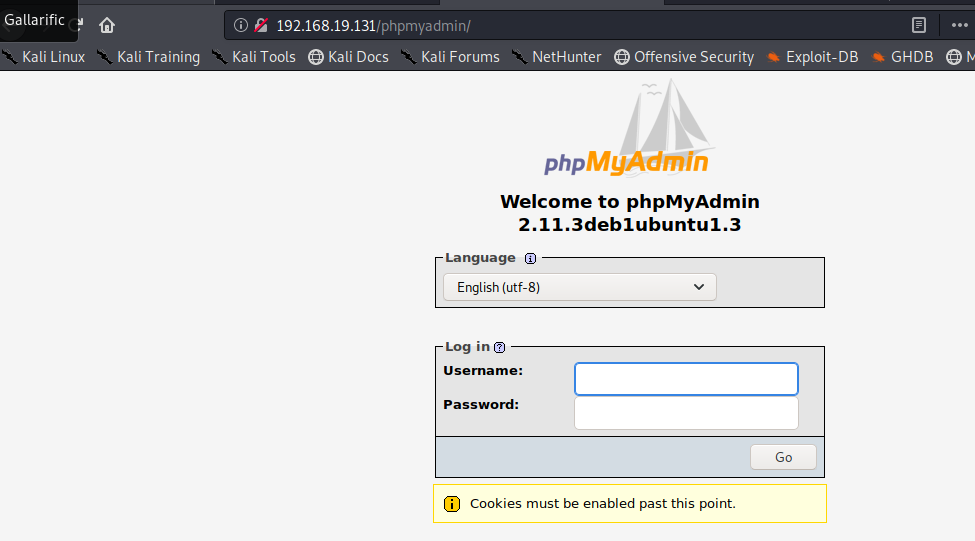
先用dirb扫到很多东西



逐一跟进，gallery好像是一个人和他养的山羊。。。



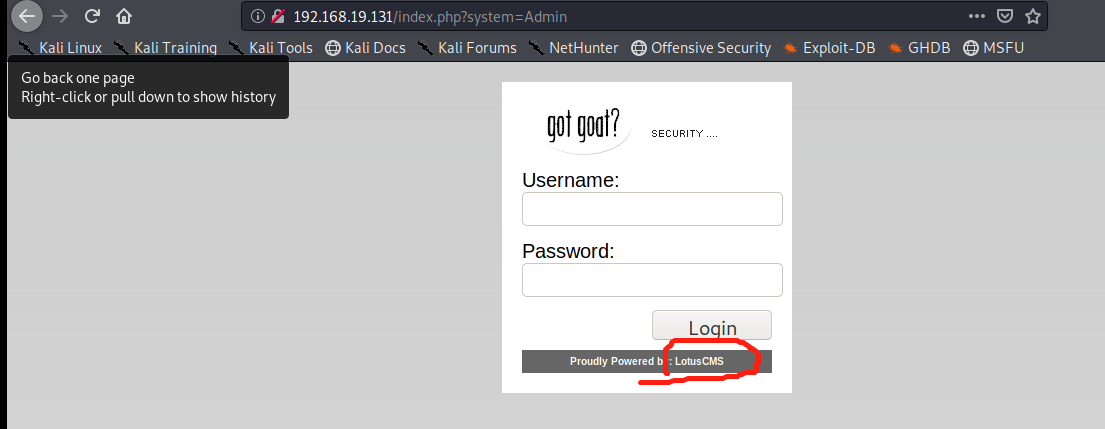
Phpmyadmin试过弱密码无法进入卒



Modules是关于一些文件，但是挖掘不出有用的信息

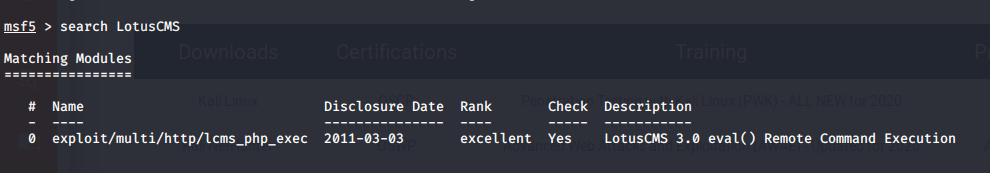


而这时回到主页面点开login,会跳转到一个页面同时下面显示是LotusCMS

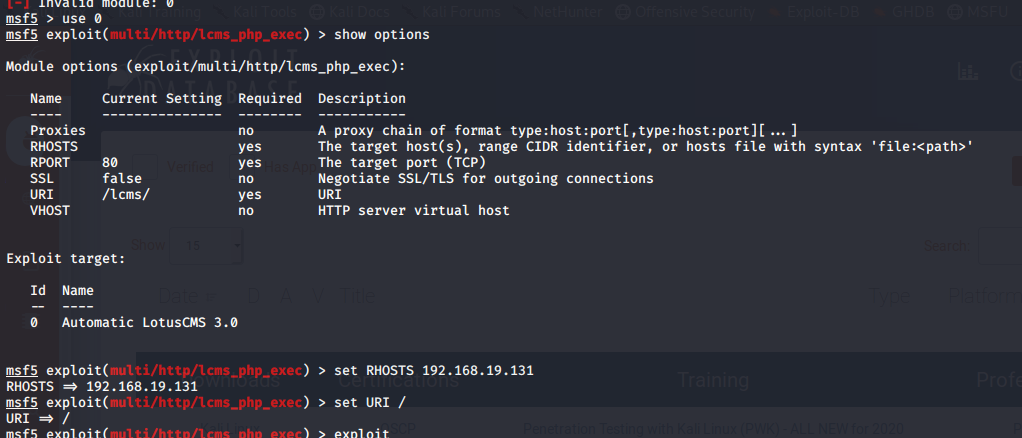


# 0x03:利用MSF获得shell

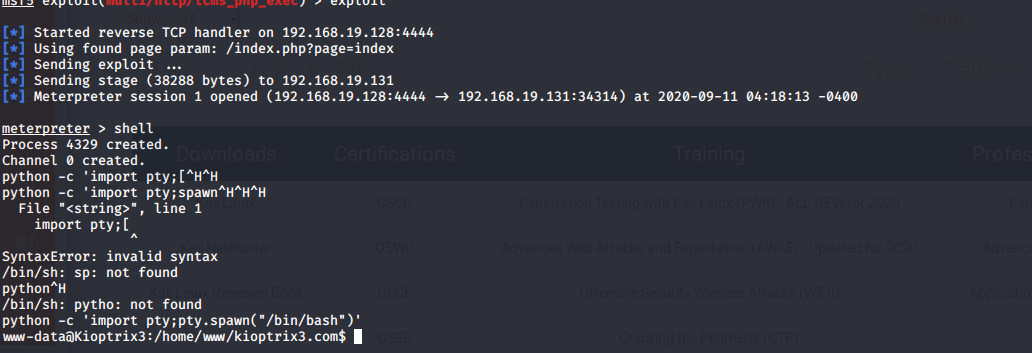
启动MSF直接用search找到一个RCE payload



先用use 0 使用这个payload,然后查看参数需要设置目标IP,顺便改一下 URI 为 /

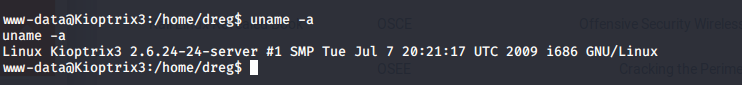


这里如果出现了meterpreter就是代表攻击成功，输入shell进入shell模式然后写一个python的交换式shell(这里手残了。。。忽略一下)

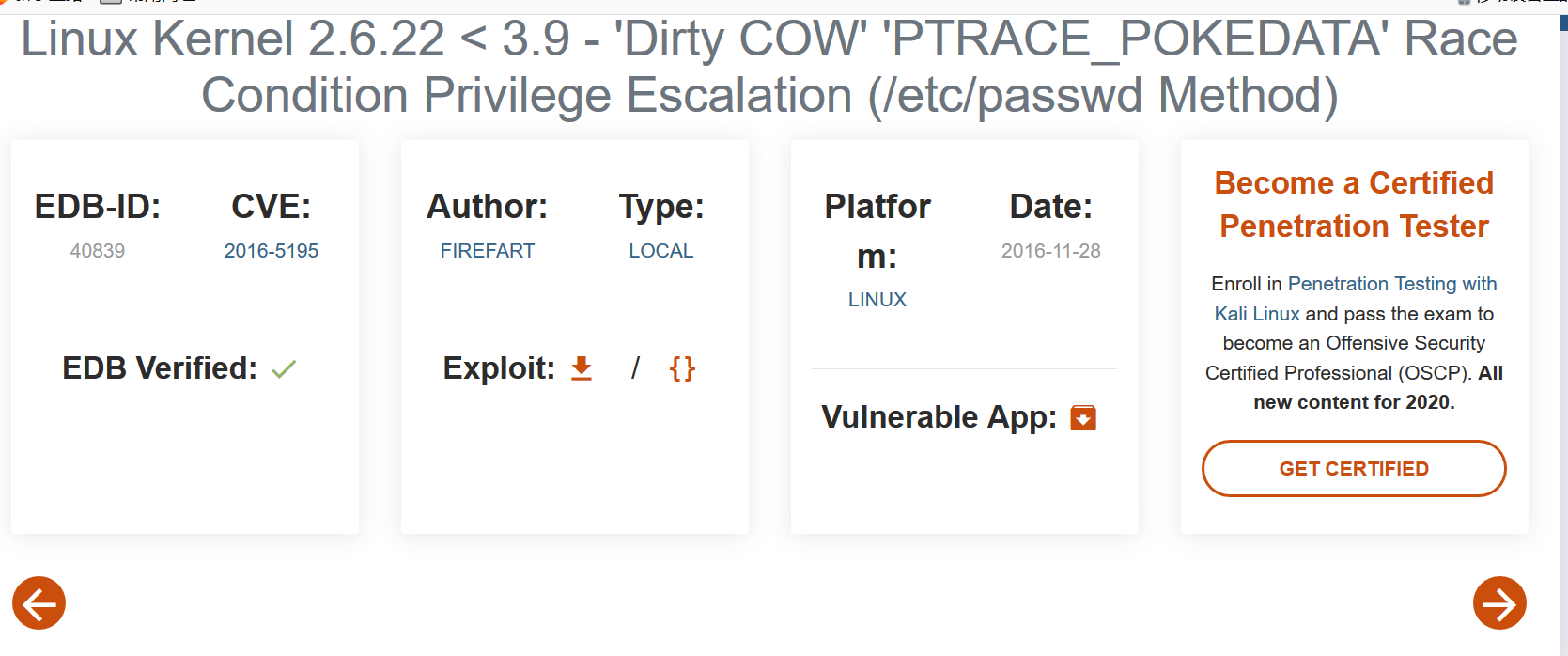


# 0x04:提权

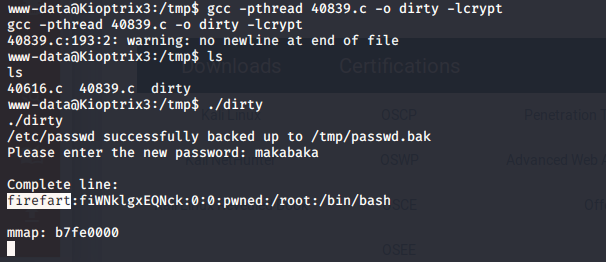
这次不用sudo -l反正也是失败，直接uname -a 查到内核为2.6



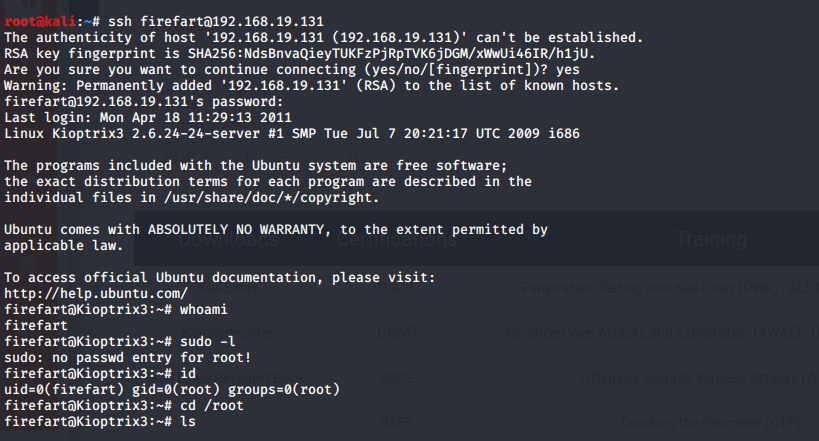
可以直接用脏牛乱拳打死



直接用gcc编译好运行输入波密码



这个时候可以用ssh，因为开了22端口用firefart作为用户名密码是makabaka登录，权限直接为root



并读到flag

