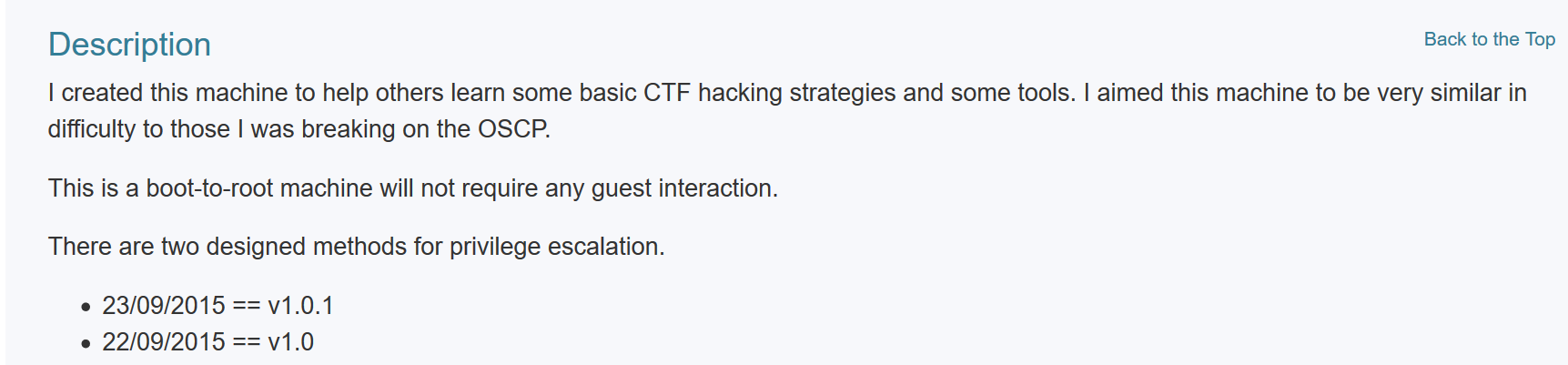
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/lord-of-the-root-101,129/>

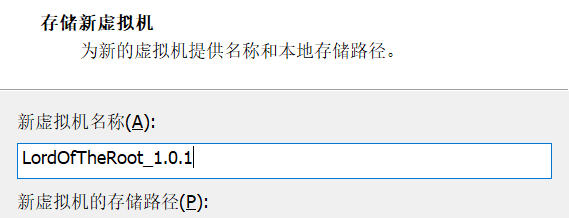
概况一波就是这个靶机跟OSCP难度非常相似emmmm感觉没那么容易把。



下载完以后是个.ova文件



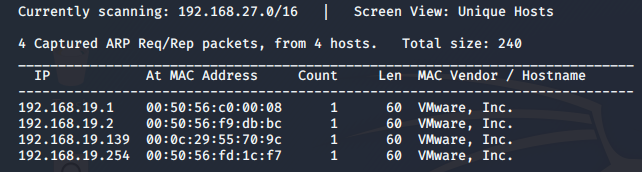
然后选择合适的地方存放就可以了，网络也默认设置成NAT模式可以直接攻击了



# 0x01:探测靶机

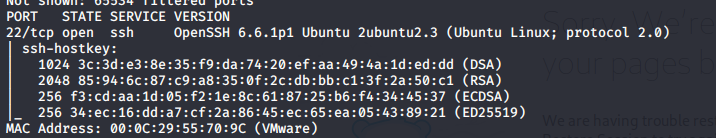
首先使用Netdiscover探测波靶机IP,排除.1,.2和.254可以确认靶机IP为192.168.19.139

命令:netdiscover -r 192.168.19.0/16

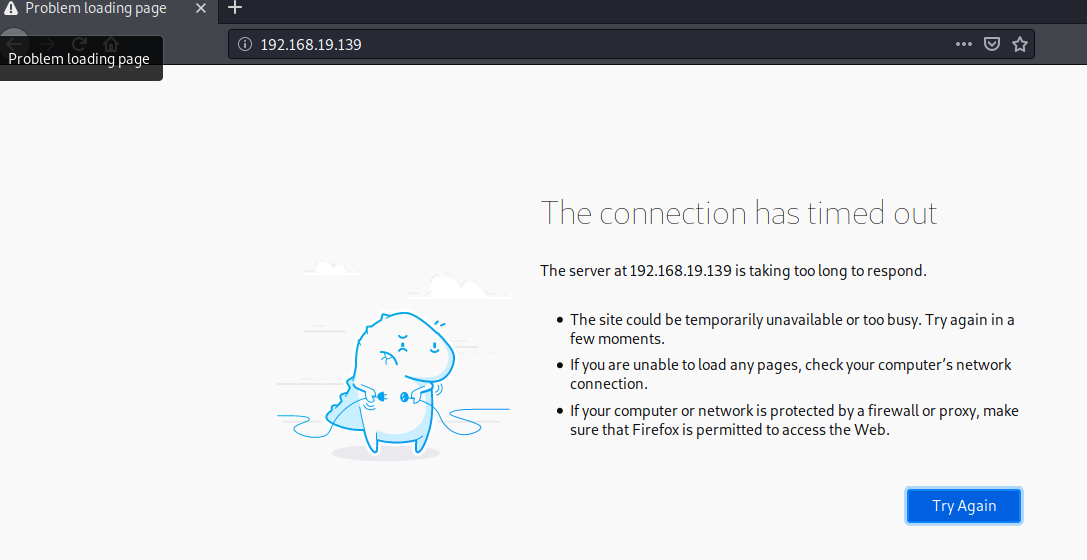


然后开始用nmap探测波端口,奇怪的是这次探测只有一个22端口

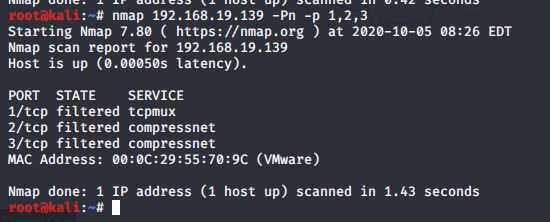
命令:nmap -A -sS -sV -v -p- 192.168.19.139



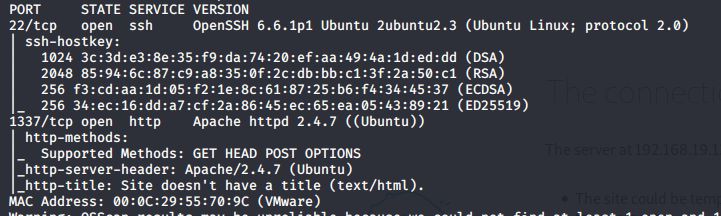
同时浏览器输入IP得不到正常页面



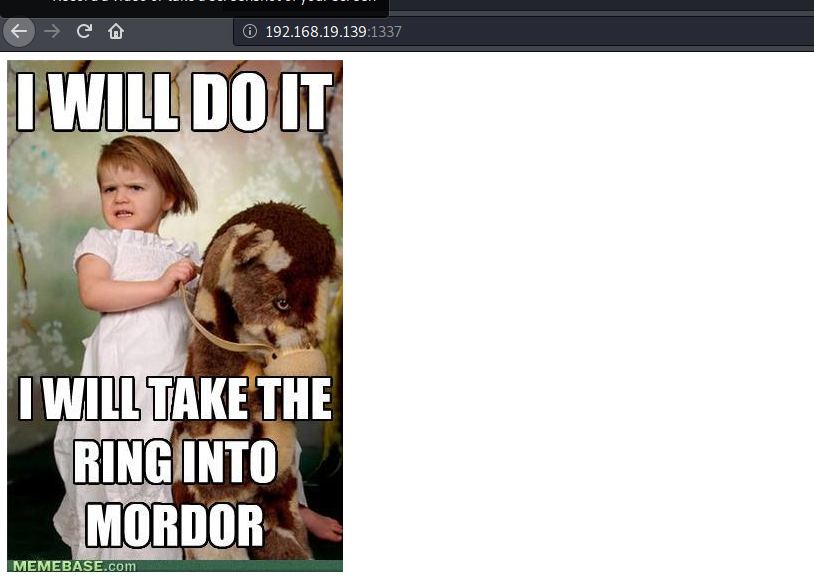
这里有2种可能，首先第一种就是靶机坏掉了，第二种可能是靶机隐藏了HTTP服务的端口。这里我更偏向于第二种可能。查了一波百度以后发现可能要用到端口碰撞技术<https://zhuanlan.zhihu.com/p/210177505> ， 不过要改进一波他的方法要变成这样敲3次才行



然后再用nmap扫描一波以后多出一个1337 HTTP服务端口

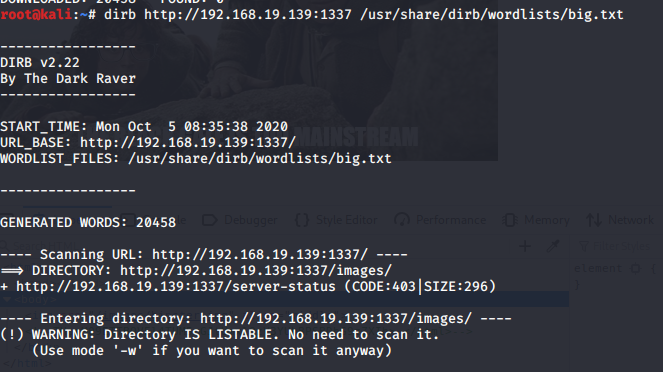


返回正常

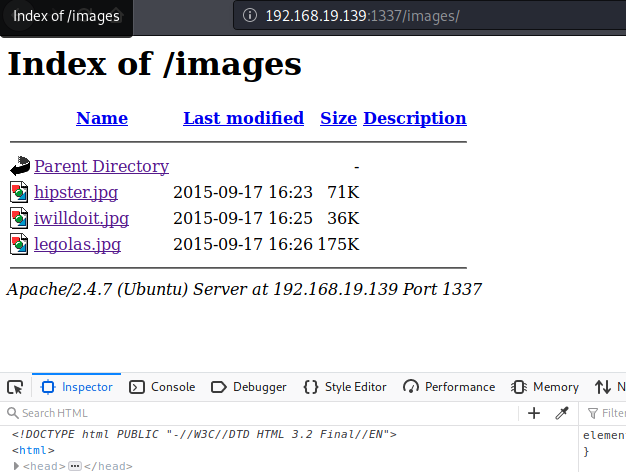


# 0x02:挖掘信息

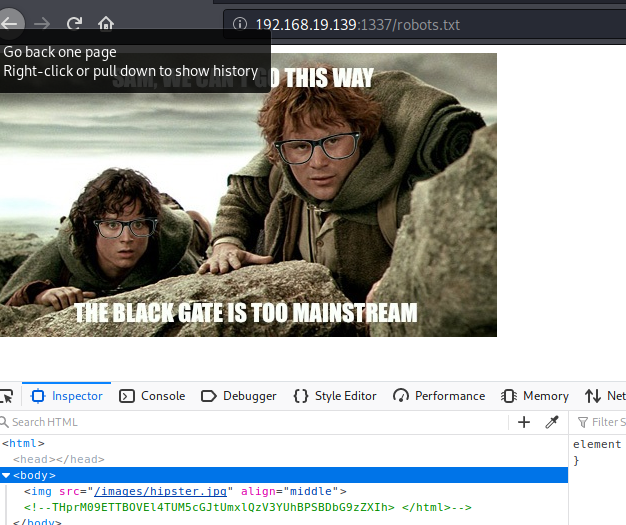
开始用dirb探探路，有点意外的是居然只扫出一个/images目录



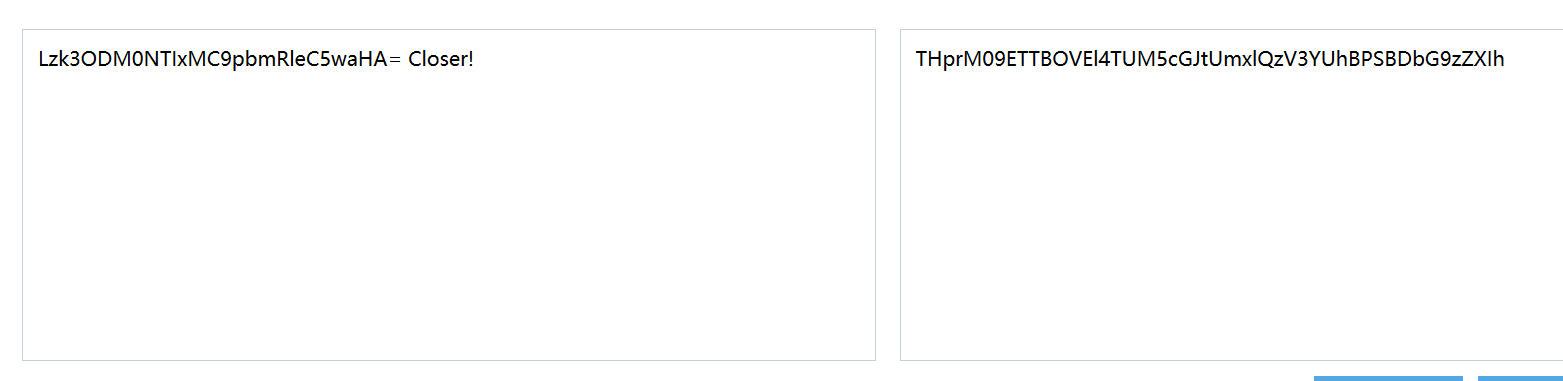
跟进一波只是3张图片而已没了。。。



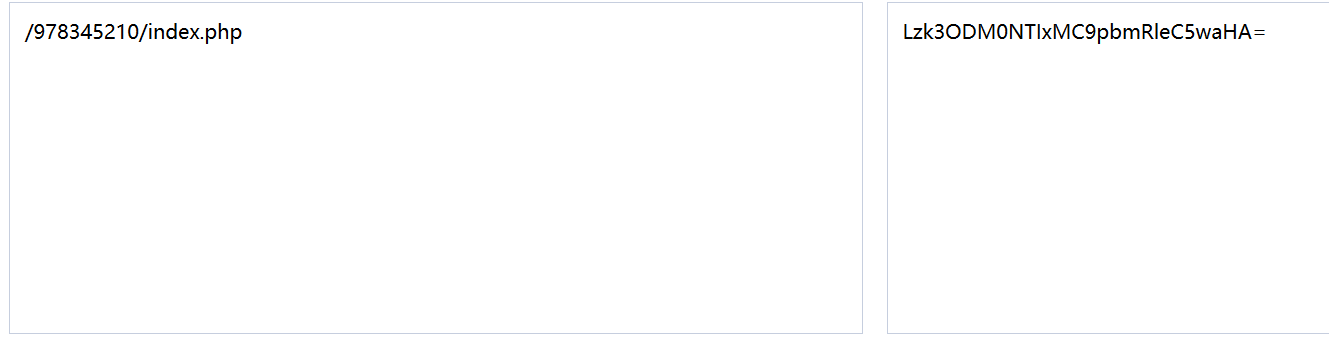
我思考着不可能呀，在手动尝试一波如/admin /robots.txt ……，最后发现robots.txt返回正常而且按住F12以后底下有串加密字符



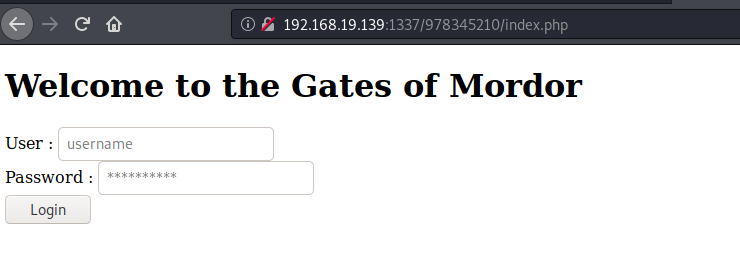
数了一波以后长度为48可以确定编码为base64



行吧继续解，再次解密得到一个目录的东西



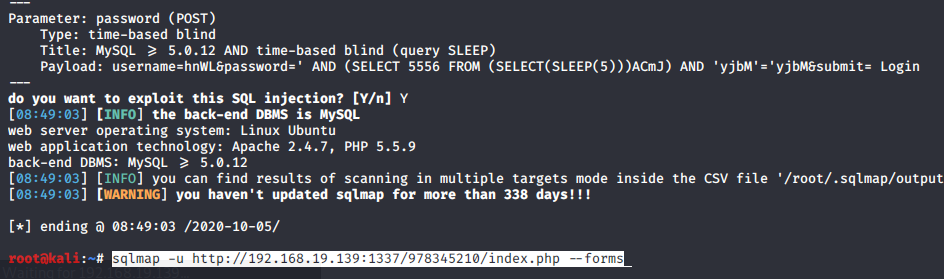
跟进一波以后确实是一个页面而且是个登录框



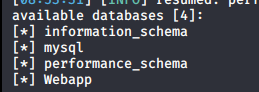
# 0x03:爆破登录框

遇到登录框通常来波burp抓包然后分别送到Intruder加载字典看看能不能碰运气和用sqlmap跑一跑，然而不知道为啥抓包跑sqlmap跑步出来只能用-u来跑

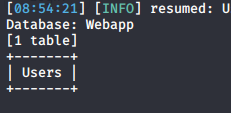
命令: sqlmap -u http://192.168.19.139:1337/978345210/index.php --forms



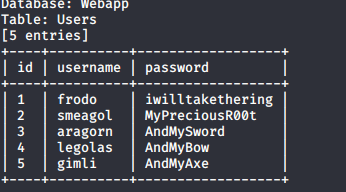
输入—dbs跑出来4个库



跟进Webapp,发现一个Users表然后跟进里面的数据

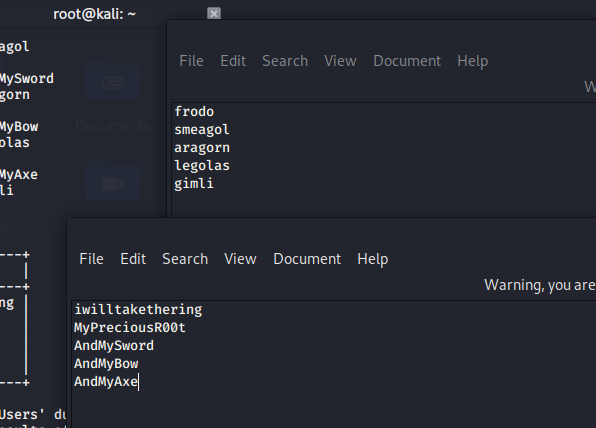


最后得到一堆账号密码数据

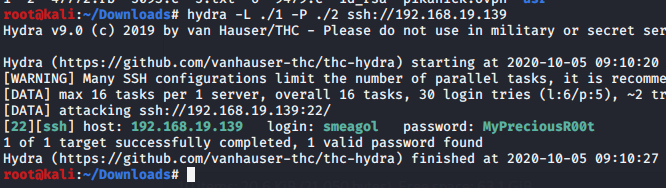


# 0x04:爆破SSH端口

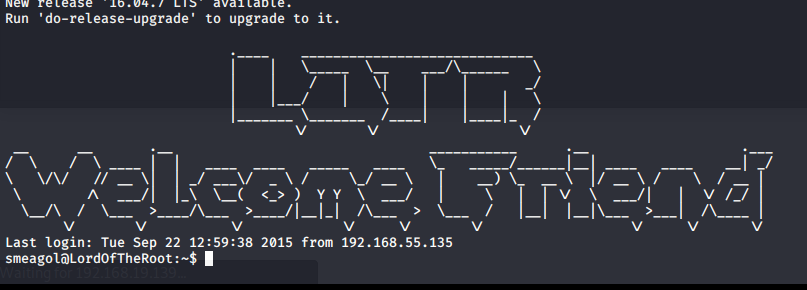
由于在探测端口的时候开了22端口，而且刚刚得到一波账号密码尝试爆破一波，先保存到文本里面



启动hydra开始爆破最后得到一个成功的账号和密码

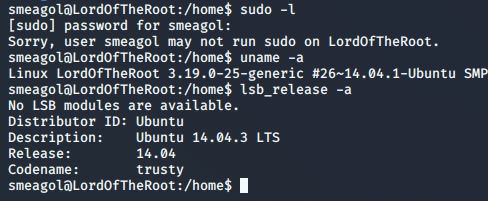


成功登录

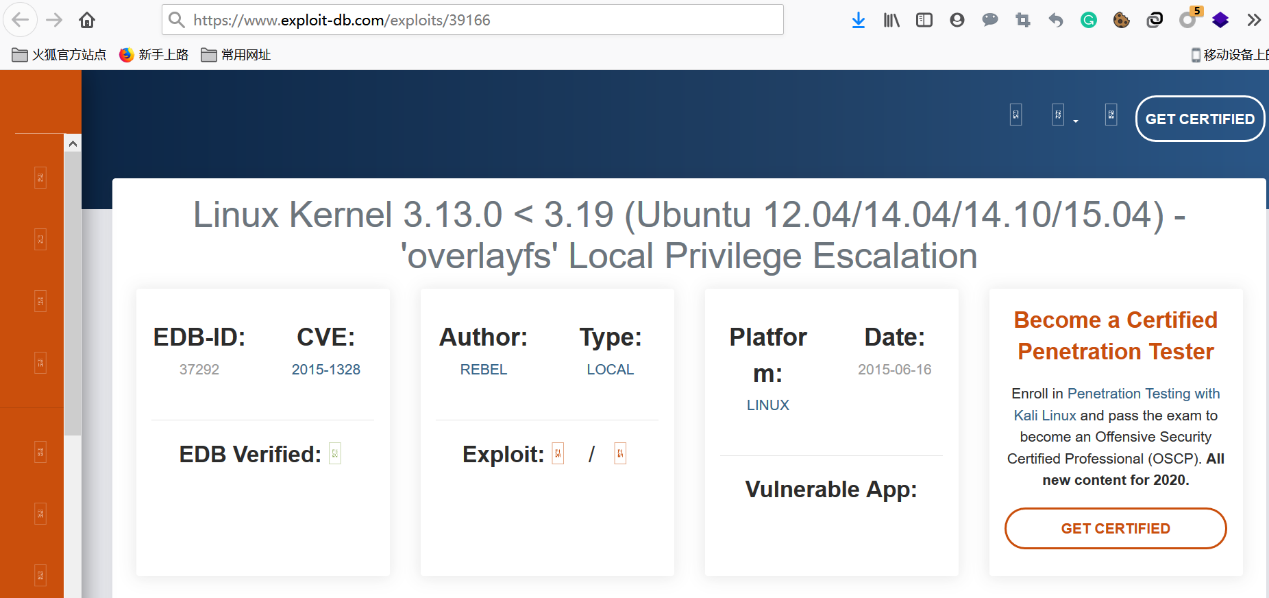


# 0x05:提权

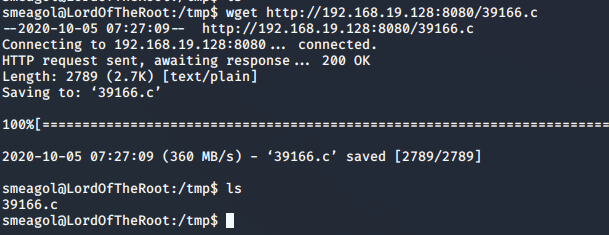
Sudo -l又失败了，只能用uname -a 和lsb\_release -a查询波版本和内核



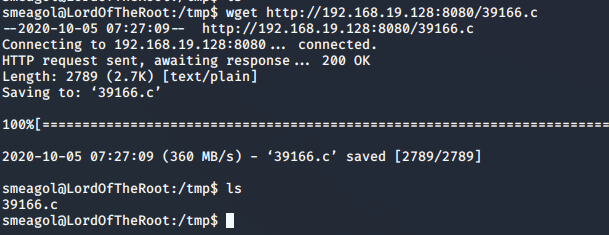
去到exploitdb找了一轮以后找到这个



下载到kali里面



开启波python共享服务，然后在靶机那里下载到/tmp目录下方便执行



运行一波以后成功变成root

