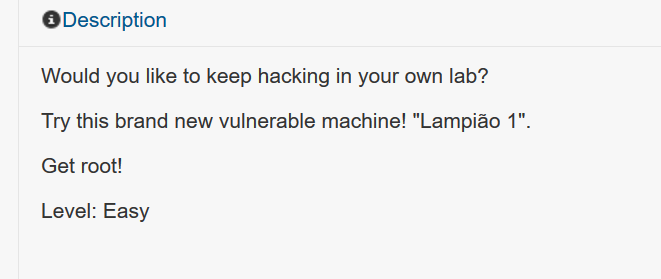
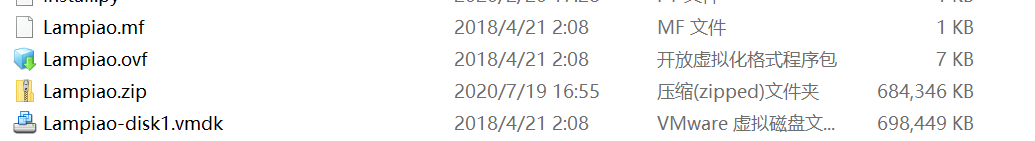
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/lampiao-1,249/>

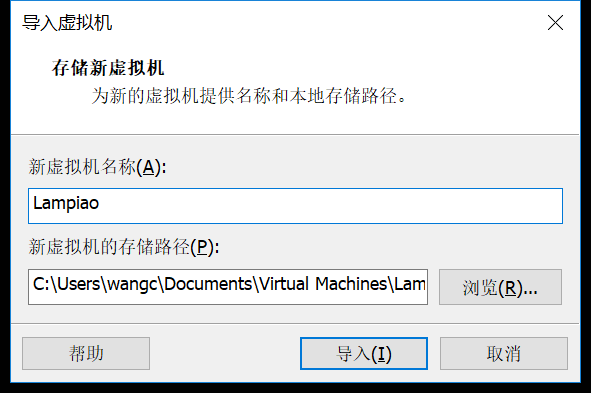
难度等级为简单目标是得到root权限



下载完以后是个zip文件解压以后有个.ovf文件



点击即可选择一个合理的位置进行安装



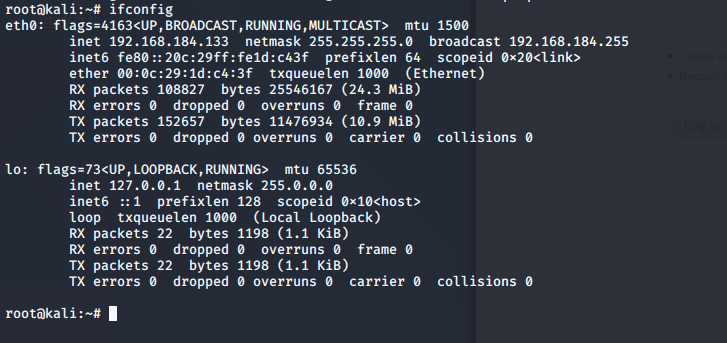
安装好以后是默认调到NAT模式运行即可



# 0x01:探测靶机

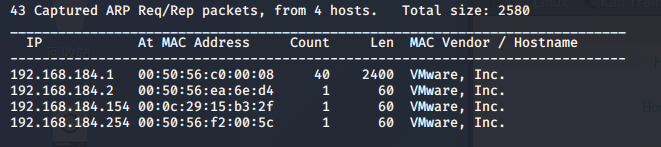
先查看一下本地kali IP

命令:ifconfig



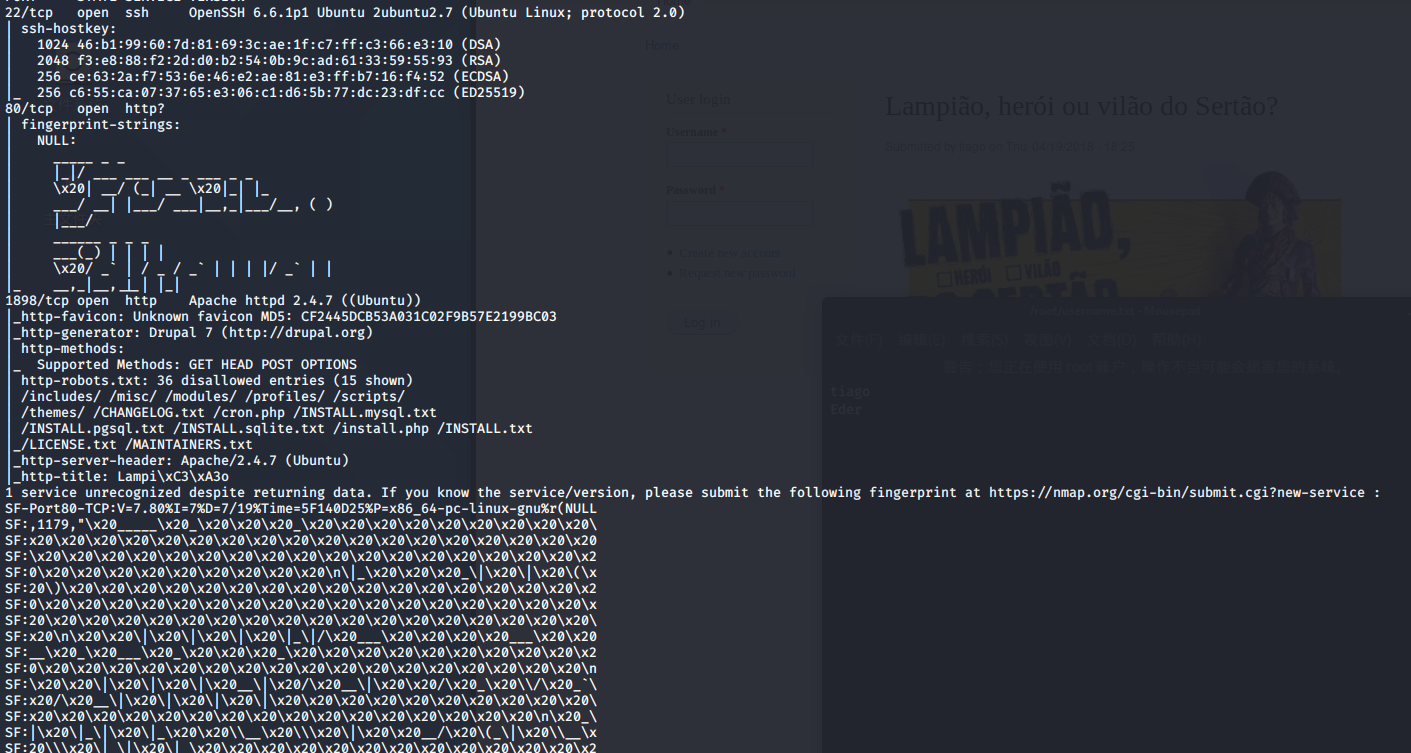
开始用netdiscover扫描C段探测靶机IP,排除.1,.2,.254默认网关可以确认靶机IP为192.168.184.154

命令:netdiscover -r 192.168.184.0/16

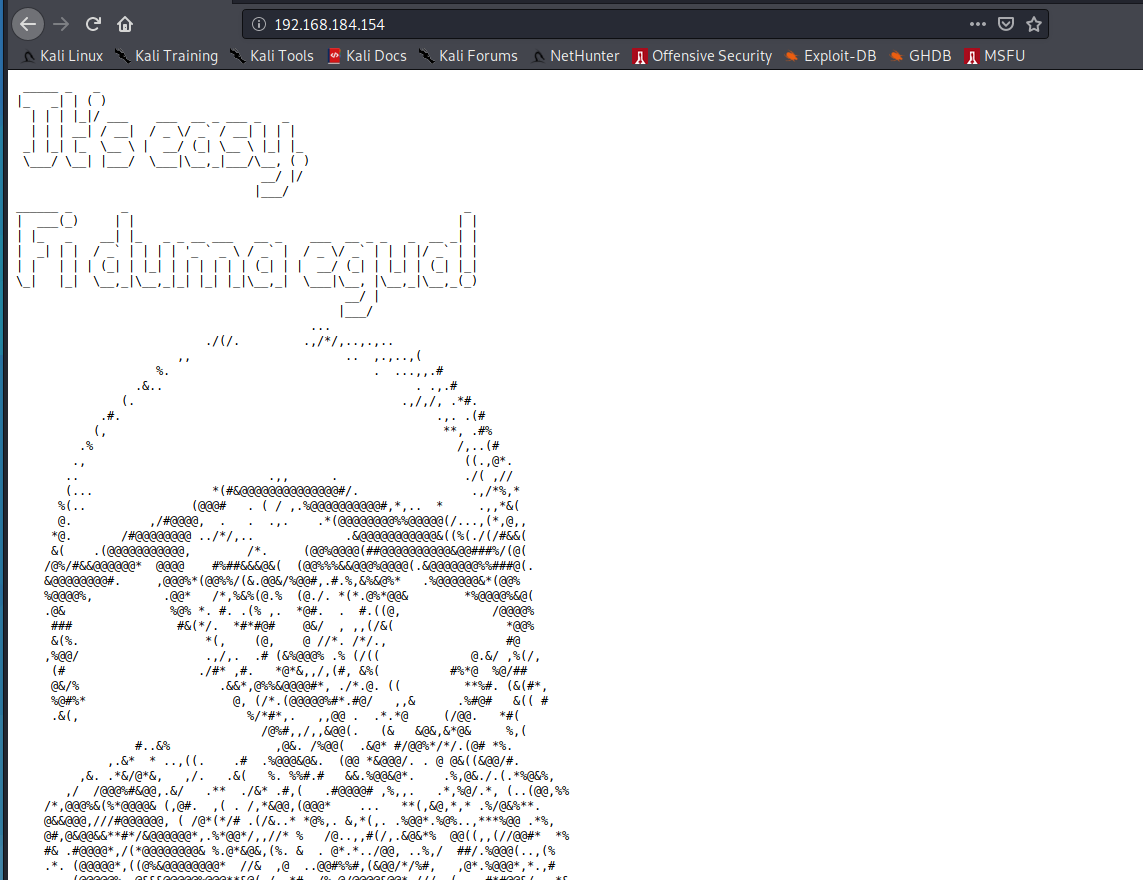


然后用Nmap探测端口,开了22，80和1898端口。由于目前没收集到什么信息，放弃22端口集中在80和1898端口上

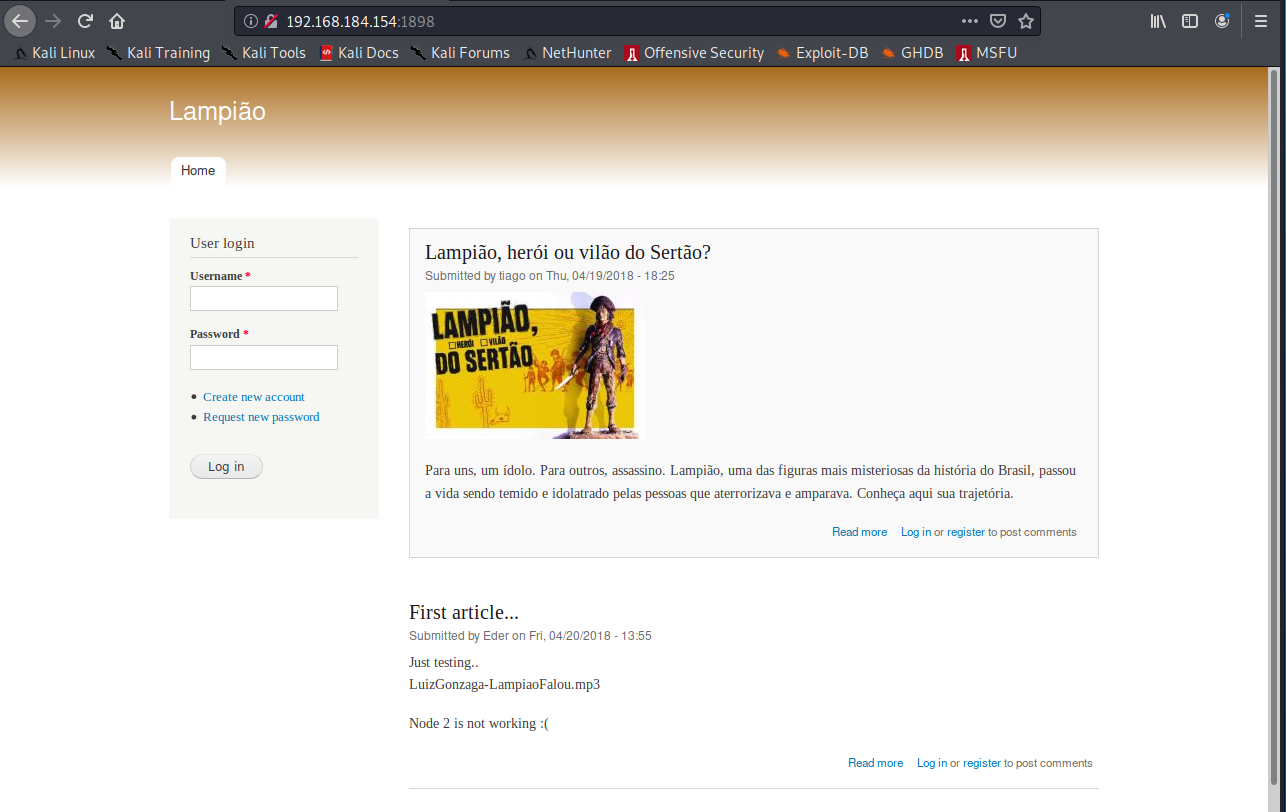
命令:nmap -A -sS -sV -v -p- 192.168.184.154



80端口只有一个图像啥都没有，放弃



而1898端口是个网站并且有两篇文章



# 0x02:漏洞挖掘

在1898端口这里有个提示submitted by tiago/Eder, 这里猜测tiago和Eder应该是两个用户名，可能是该网站的或者是SSH端口可以用到的。同时在这个网页里有很多信息猜测可能有密码藏在这里



先把两个用户名放在username.txt里面



然后用cewl爬虫该网页信息放到word.txt文本里面

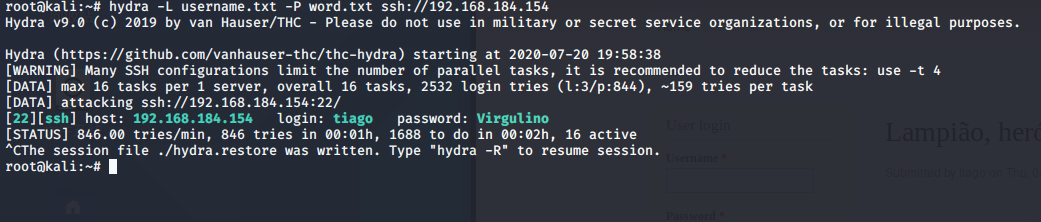


接下来就开始用hydra尝试爆破22端口最后可以爆出一个用户名和密码出来

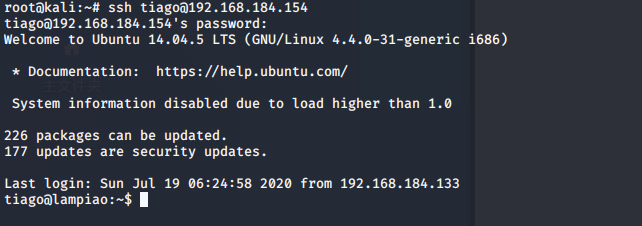
命令: hydra -L username.txt -P word.txt ssh://192.168.184.154

用户名:tiago

密码:Virgulino

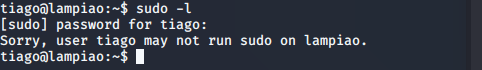


尝试用ssh，登录成功

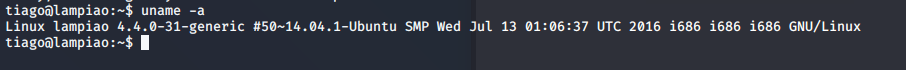


# 0x04:提权

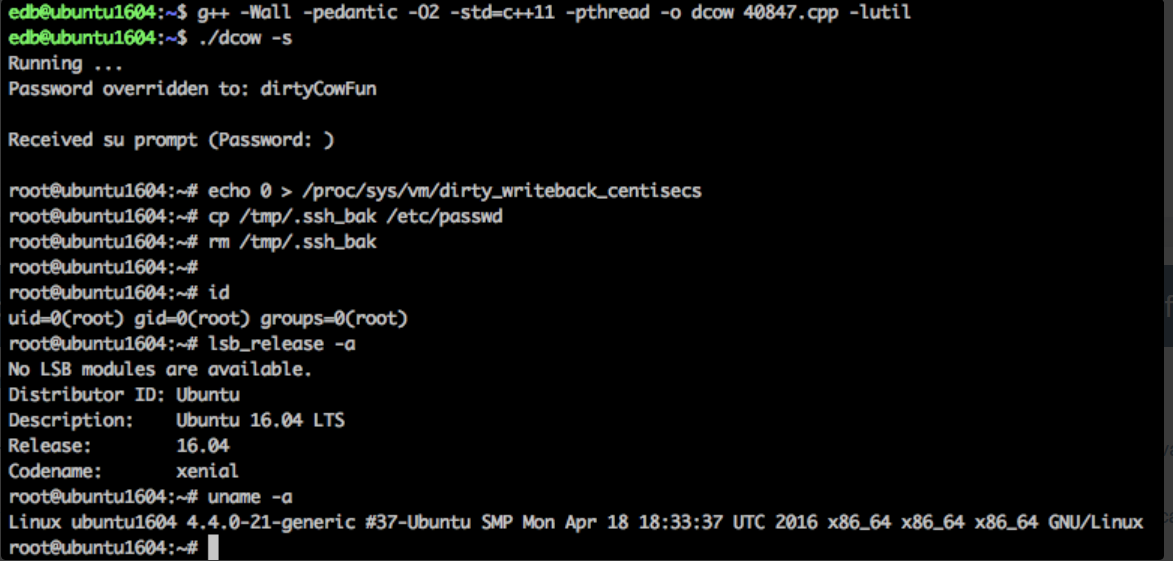
由于目标是获取root权限，先sudo -l一波，发行运行不了



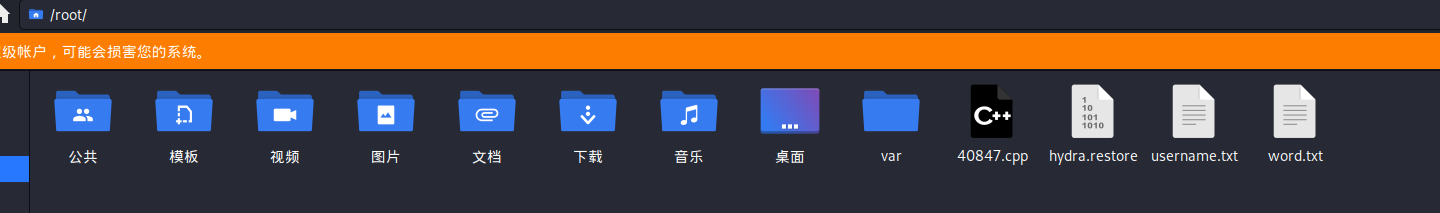
尝试uname -a ,成功查看到版本信息



通过在必应查询到该EXDB有payload <https://www.exploit-db.com/exploits/40847>，同时在底下附带的照片有使用方法

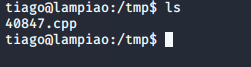


下载完以后先复制到kali的root目录下



用scp命令成功传到目标服务器上





最后按照照片上提供的方法，成功获得root权限并且得到flag

