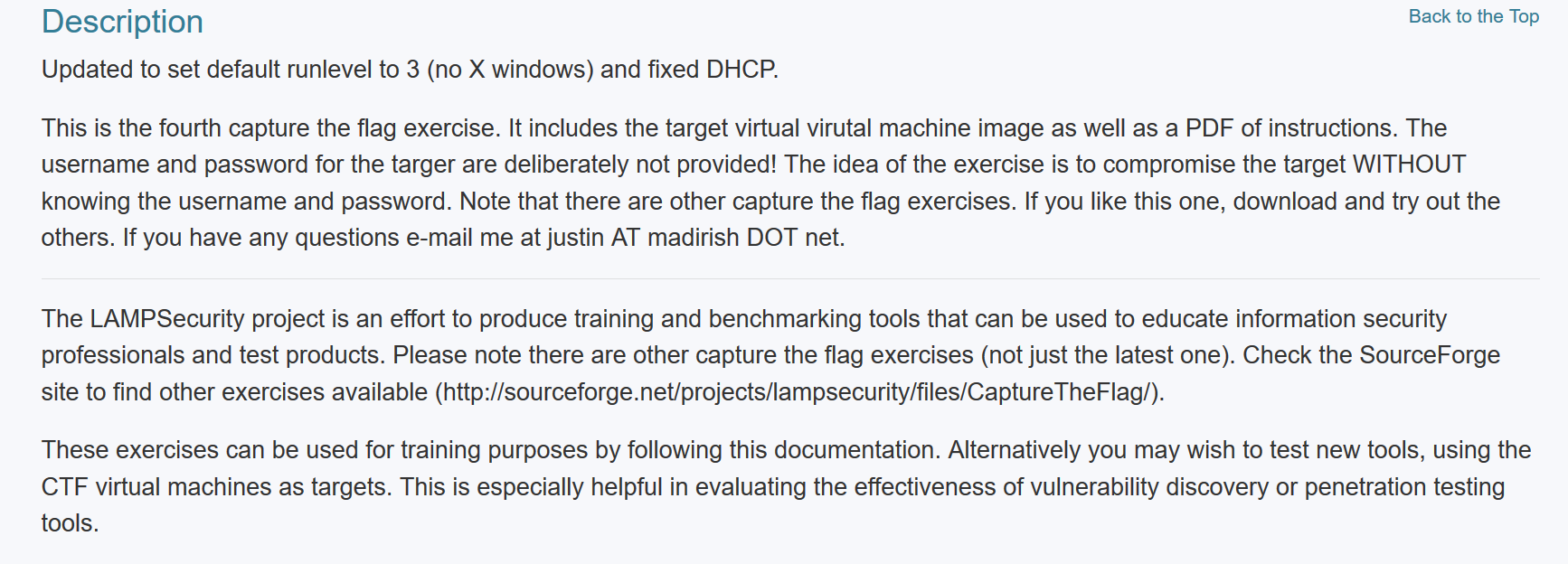
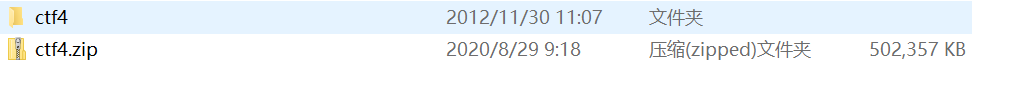
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/lampsecurity-ctf4,83/>

今天来玩点反常点的东西，这是11年前的靶机，目标就是得到root权限



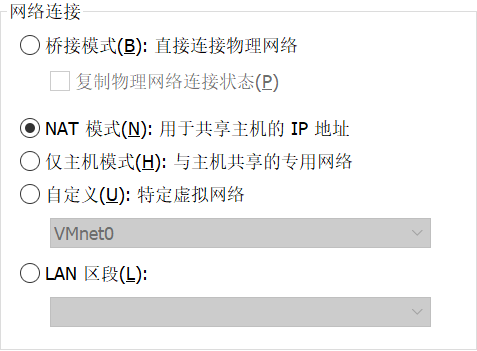
下载以后解压



然后点击.vmx就可以直接安装好了



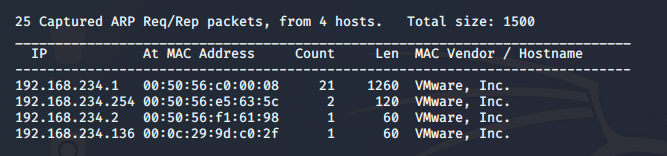
不过还是要调回NAT模式



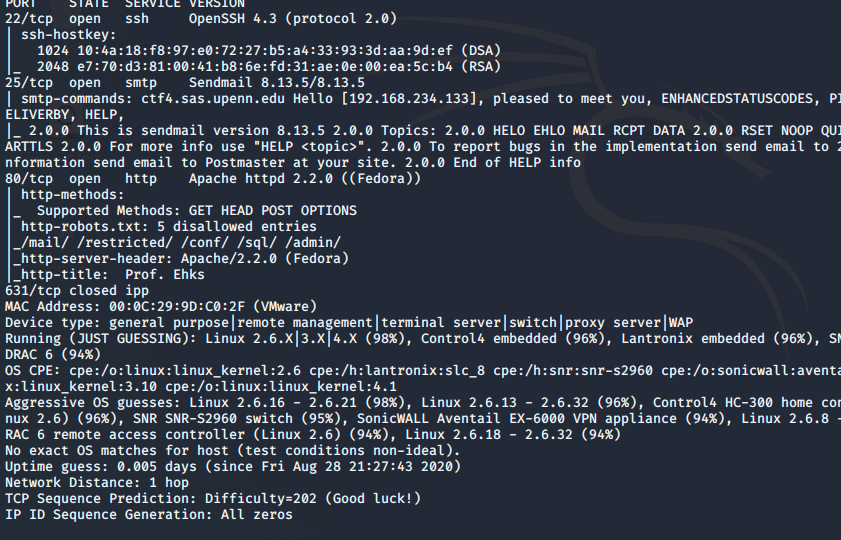
# 0x01:靶机探测

还是先用netdiscover探测一波先，排除.1,.2和.254可以确认靶机IP为192.168.234.136

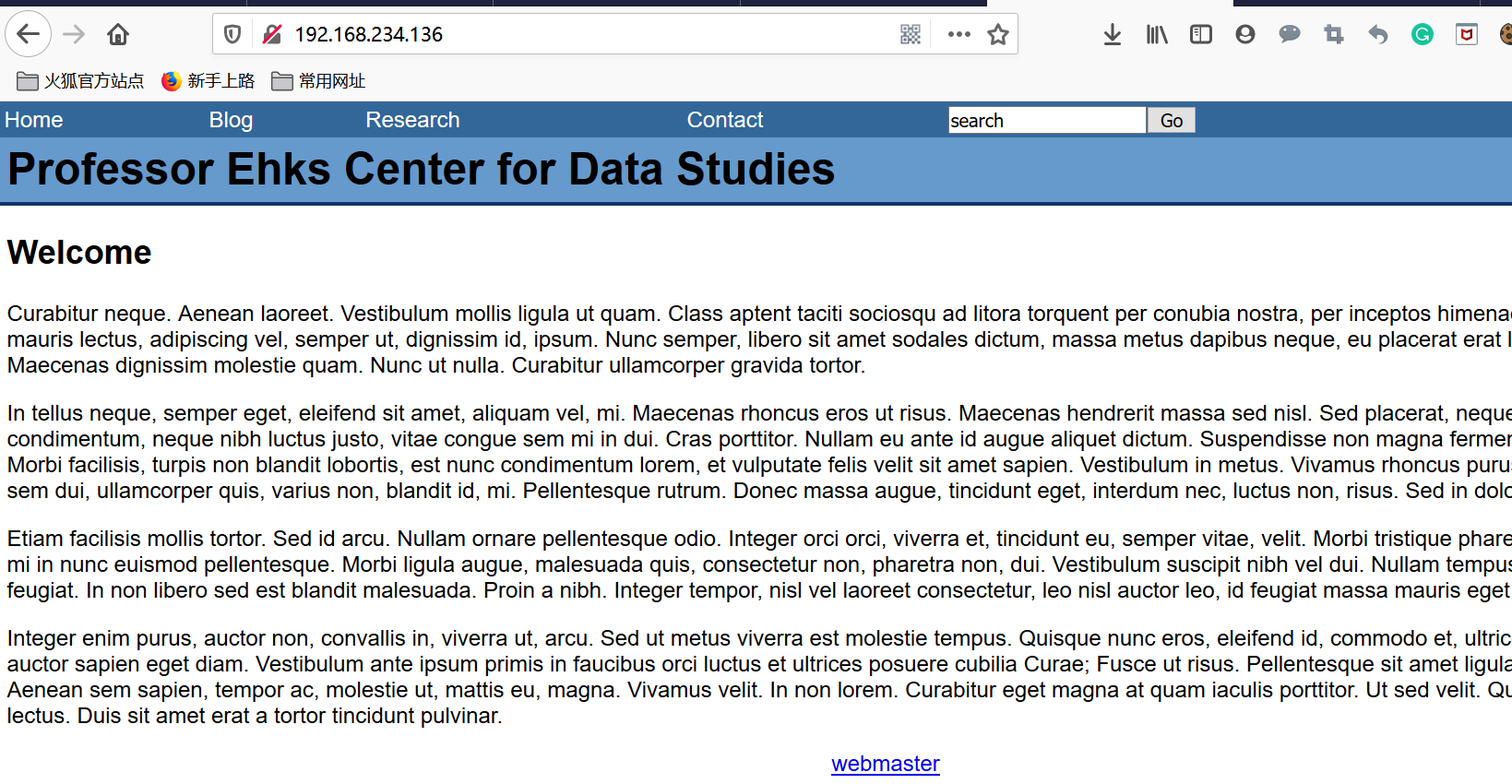
命令:netdiscover -r 192.168.234.0/16



然后用nmap探测波端口，主要开了22，25，80和631

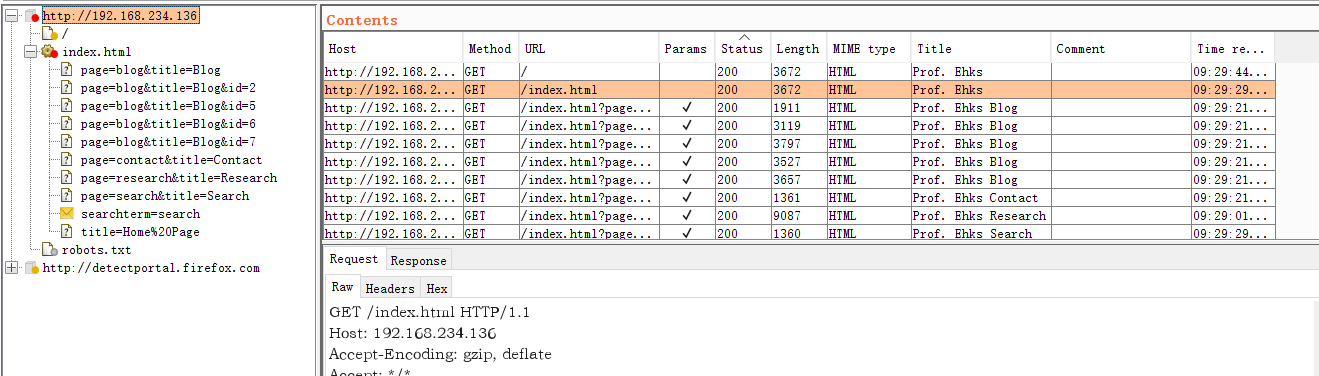


输入一波IP可以正常回显，开搞

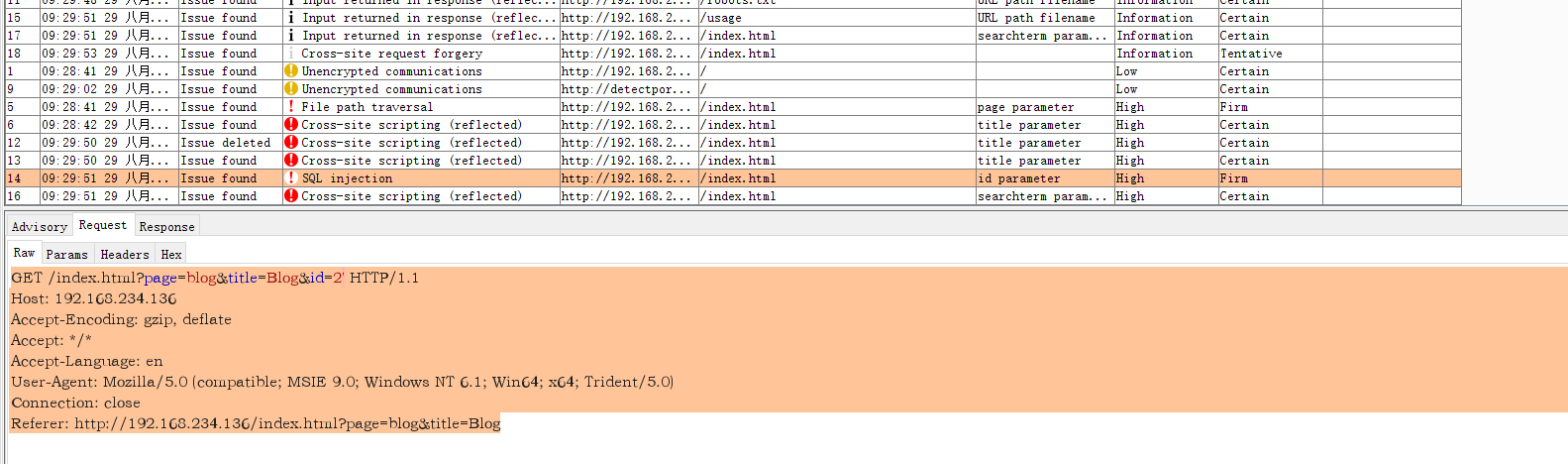


# 0x02:挖掘漏洞

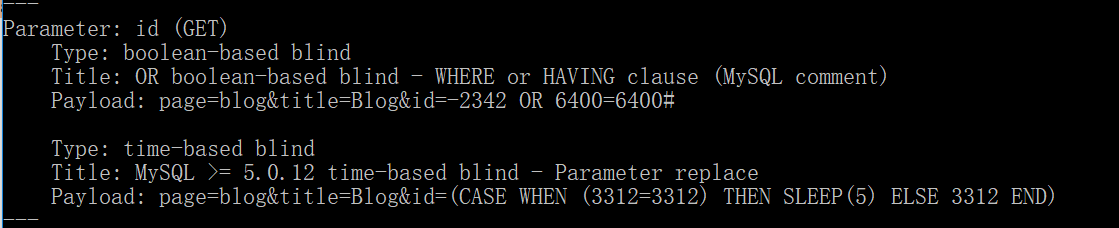
来一波降维打击，用Burp的activescan看看能不能扫出点什么，先抓个包，然后送去spider



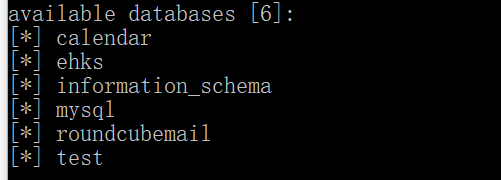
接着就是送去active scan了，芜湖直接扫出一堆XSS和一个SQL



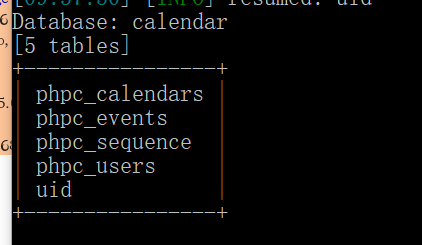
保存文本送到sqlmap直接跑出来



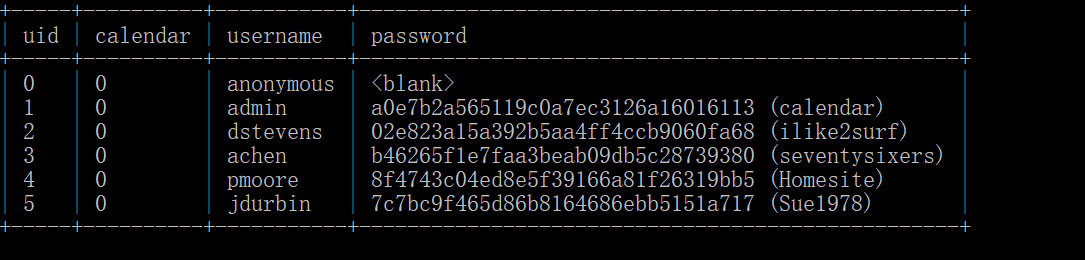
用—dbs查看数据库



这里我选择calendar数据库然后—tables跑点表出来

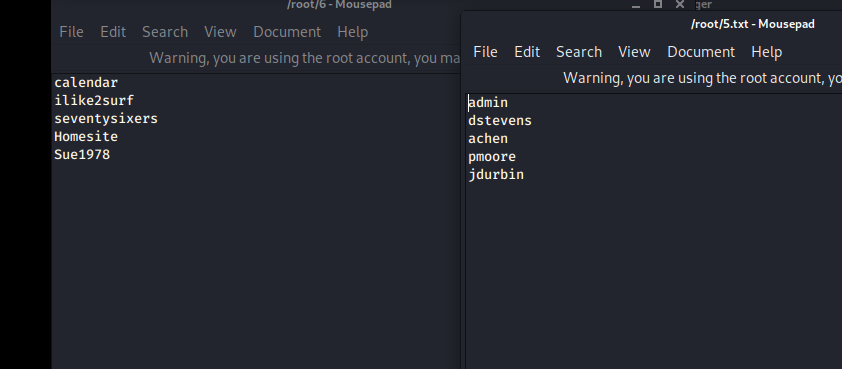


噢这里看到有个users果断选择这个表然后—dump跑里面的数据(注:平时挖掘网站漏洞请不要用—dump,这是违法的)果断跑出admin和其它用户数据出来还顺便包解密了芜湖

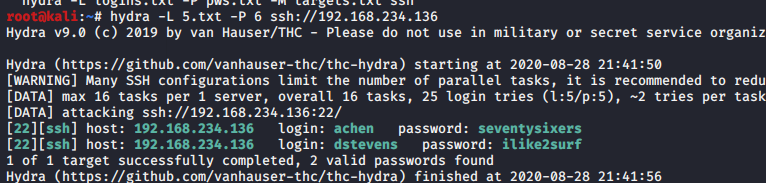


# 0x03:爆破SSH端口

由于之前用nmap探测了波端口开了22端口尝试保存刚才得到账号密码

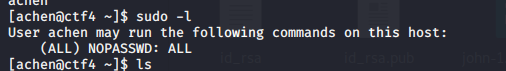


然后就用hydra开始爆破得到两个账号



# 0x04:提权

提权其实很简单用sudo -l查看一波，直接是all



直接sudo su root可以无密码切换，可能是11年前的靶机还没设置flag。。。。。

