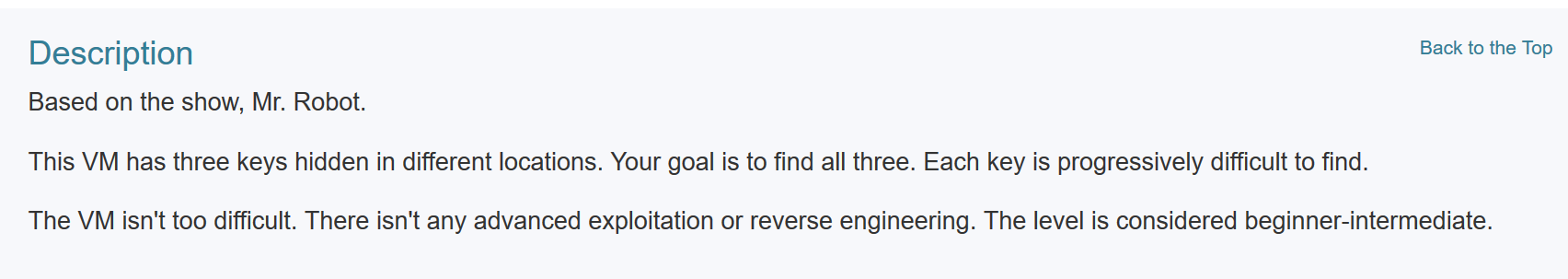
# 0x00:下载靶机

下载链接: <https://www.vulnhub.com/entry/mr-robot-1,151/>

该靶机有3个keys在不同的位置，新手到中等级别



下载完以后是个.ova文件，双击点开后选择一个位置存放

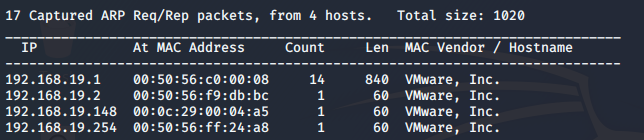


调回NAT模式就可以运行了



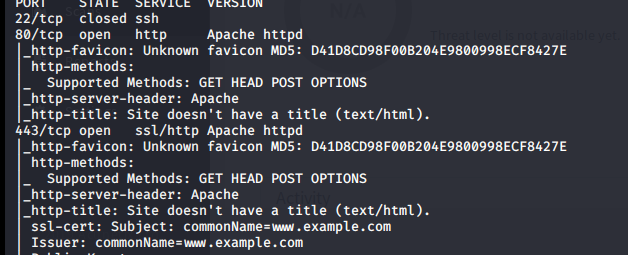
# 0x01:靶机探测

先用Netdiscover确定靶机IP，排除.1,.2和.254可以确定靶机IP为192.168.19.148

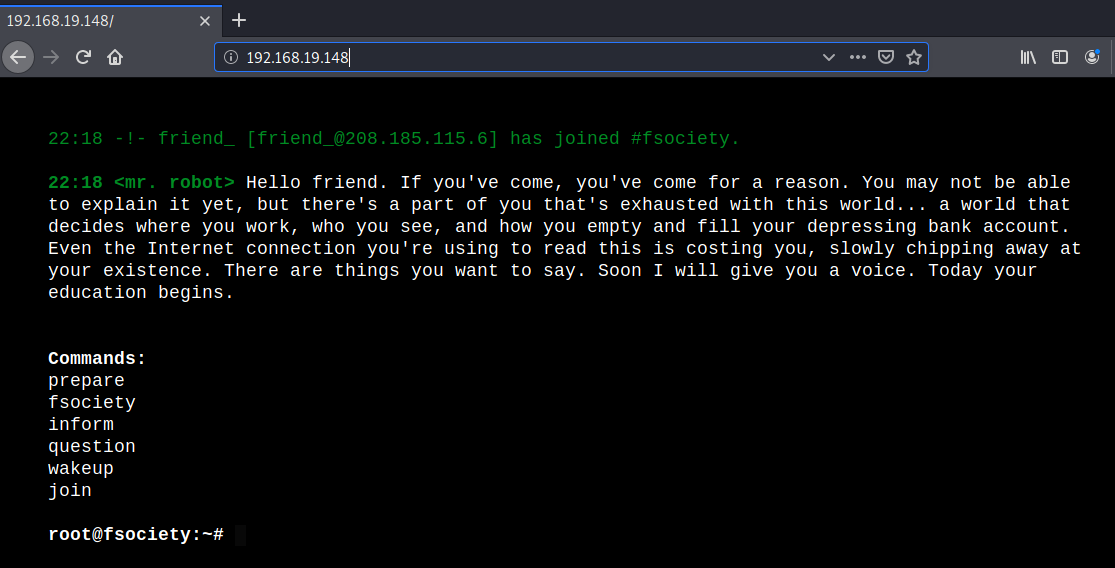


然后用nmap探测了一波端口这次开了22，80，443

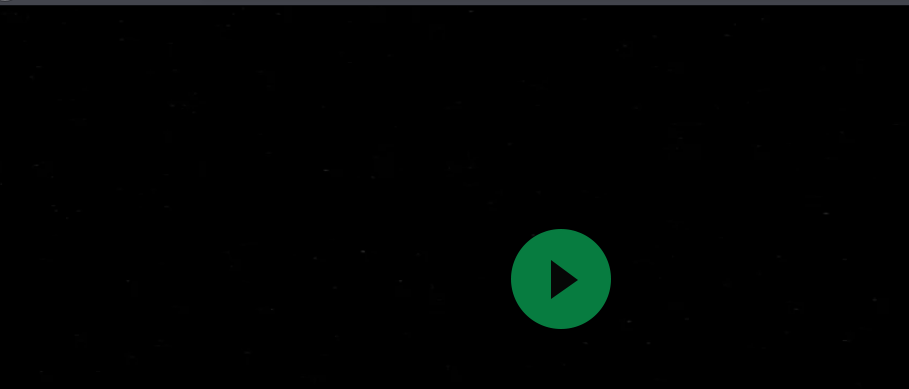
命令:nmap -A -sS -sV -v -p- 192.168.19.148



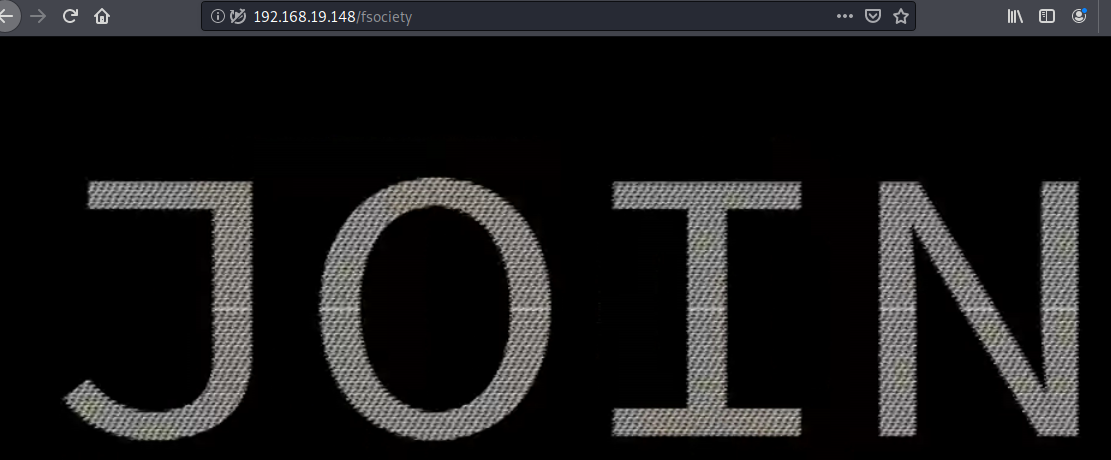
输入IP会发现这个界面有点小酷，有prepare, fsociety, inform, question, wakeup,和join命令



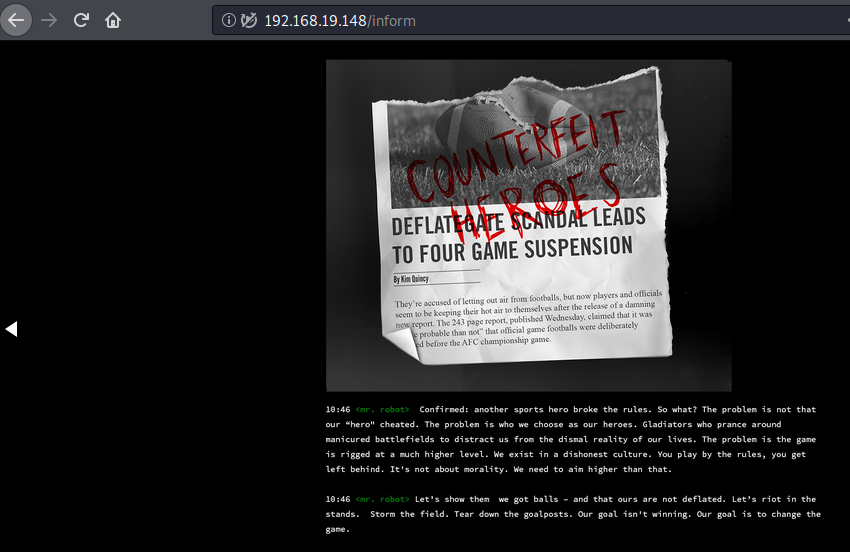
Prepare是看一段视频



Fsociety=视频



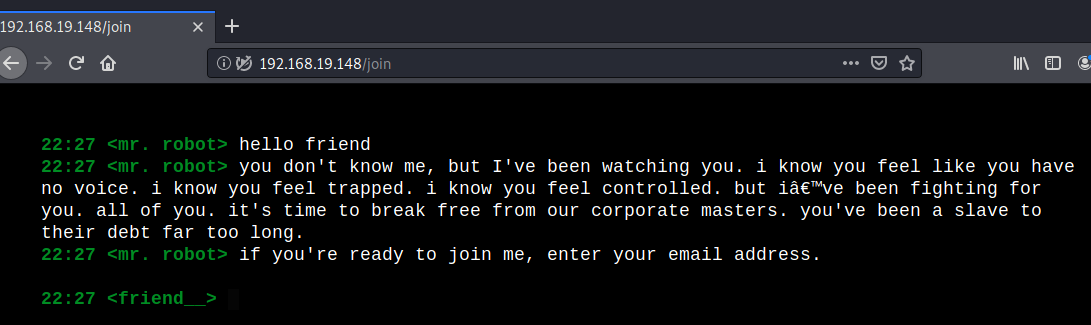
Inform=图片



Question=图片

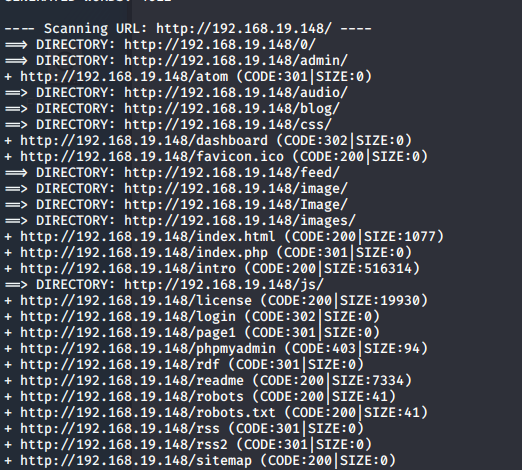


然后join是要输入邮箱???有点奇怪

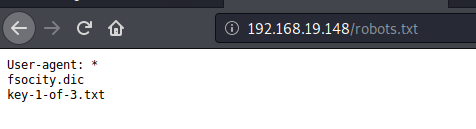


# 0x02:挖掘信息

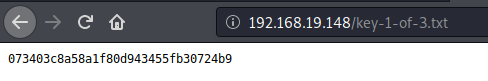
这里用dirb探探路，结果有点离谱扫的东西有点多



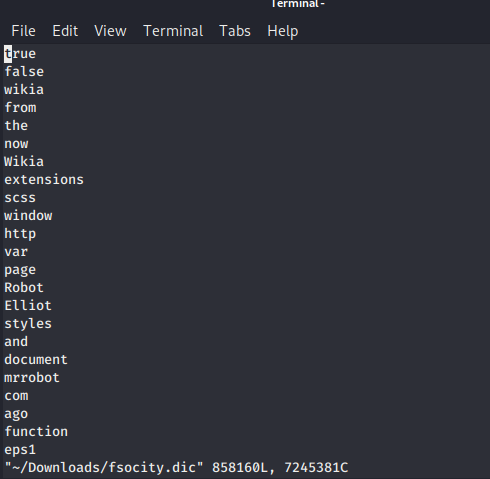
这里还是先决定访问一下/robots.txt发现2个有用的东西，一个是1个key,另外一个是fsocity.dic



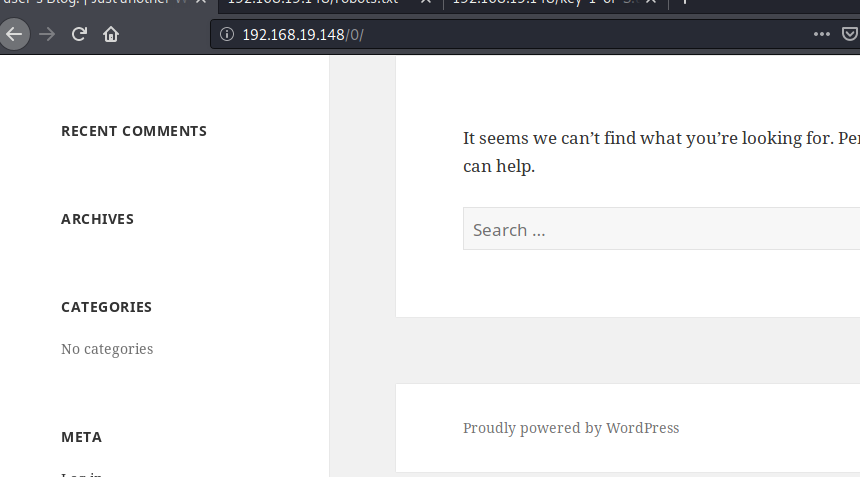
跟进一下得到第一个Key



下载另外一个文件是个字典，等下可能会用到



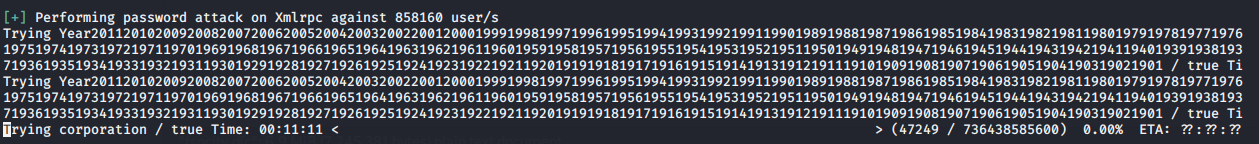
然后还发现了一个wordpress的站点



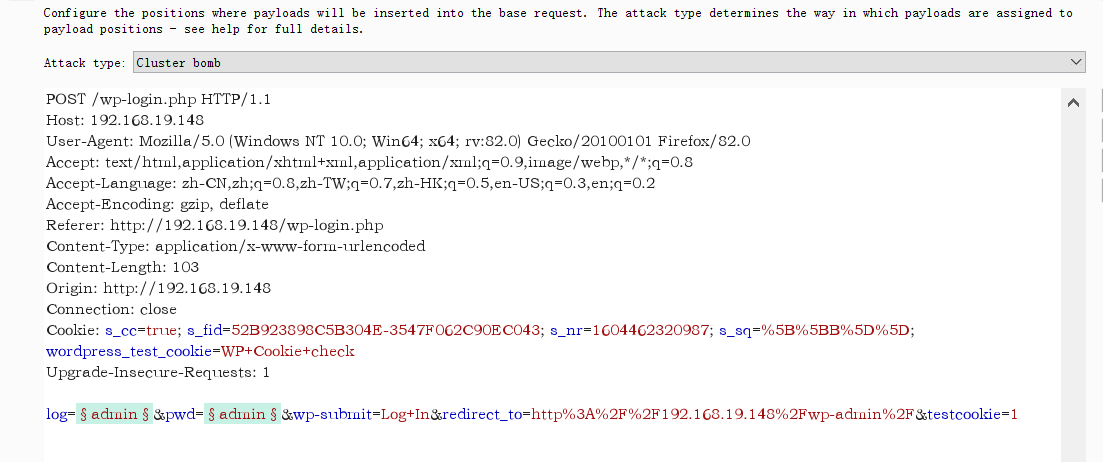
# 0x03尝试爆破后台

这里由于是个wordpress的站，同时我们得到一个字典，所以想尝试爆破一波后台在kali这里用wpscan爆破

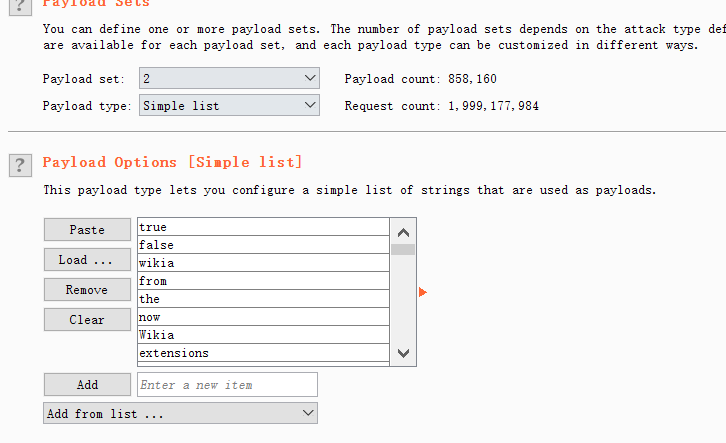
命令: wpscan --url http://192.168.19.148 -P /root/Downloads/fsocity.dic -U /root/Downloads/fsocity.dic



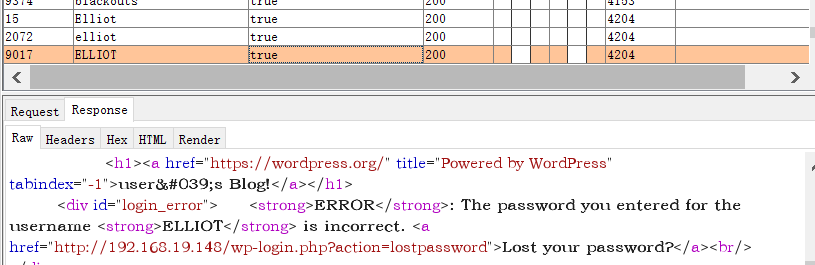
然后在BURP这里在抓包开一个Intruder,选择log 和Pwd那里变绿即要爆破的地方，攻击模式改为cluster bomb



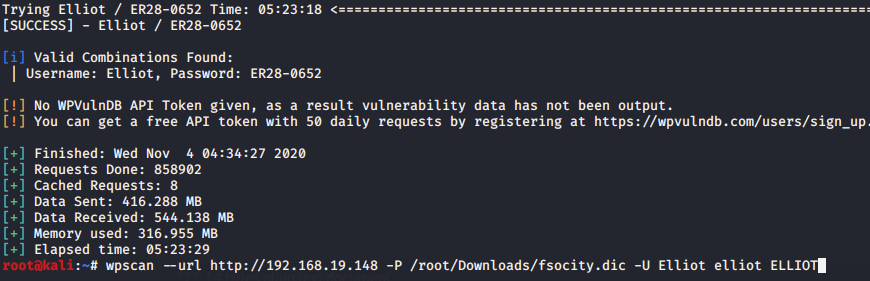
然后payload把刚才下载好的字典传上去(注意payload set 1和2都要传字典)



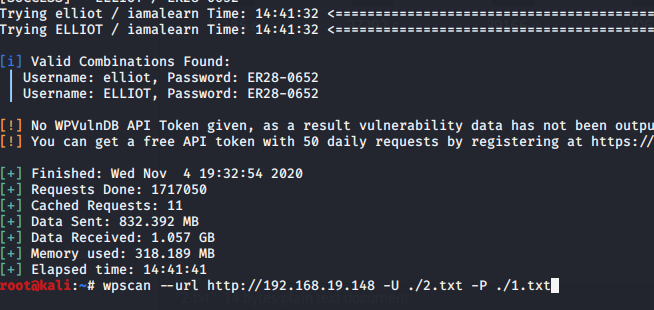
由于爆破了好久等的时间也太长了这里研究了一下发现有3个长度不一样的用户为Elliot,elliot和ELLIOT它们的返回信息有一个当前用户输入的密码不正确而其它大部分包返回都是无效用户这样



可以缩小一波范围说实话，要不然可以爆破一下午，这里用wpscan爆破但是失误了，原本我想偷懒三个用户直接连在一起算了，结果只爆破了一个用户就用了5个小时。。。。。

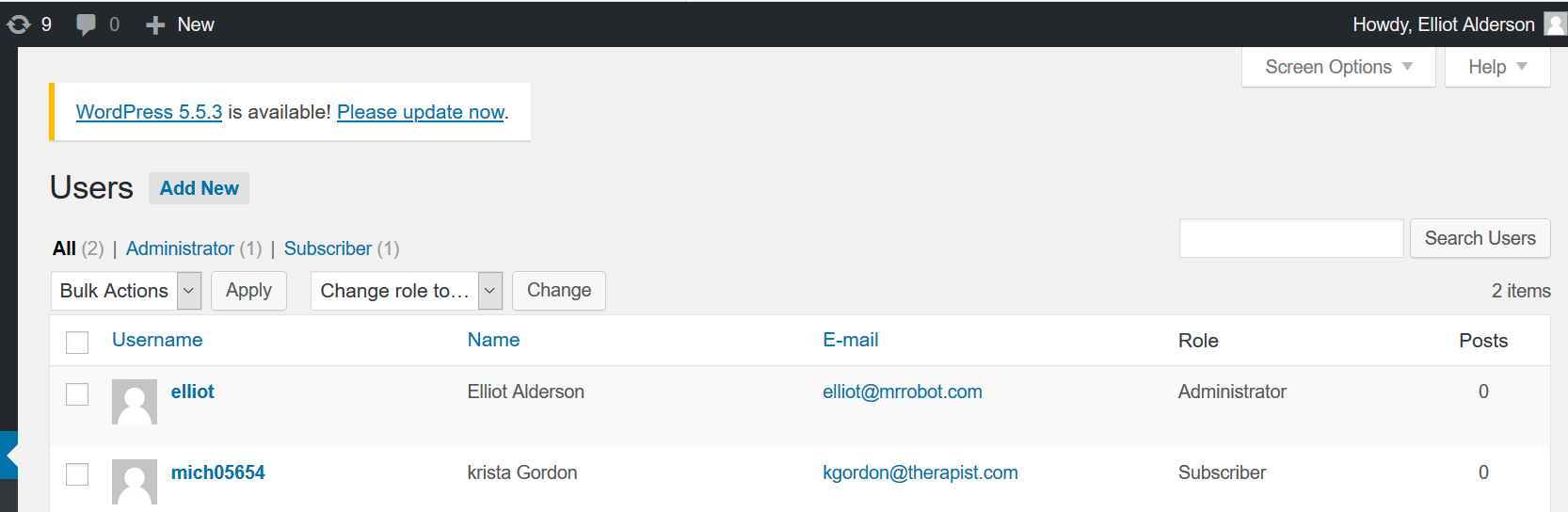


这次学聪明了，干脆把账号，密码放到文本。爆破了差不多10多个小时，最后才知道三个用户的密码都是一样的，心态爆炸。

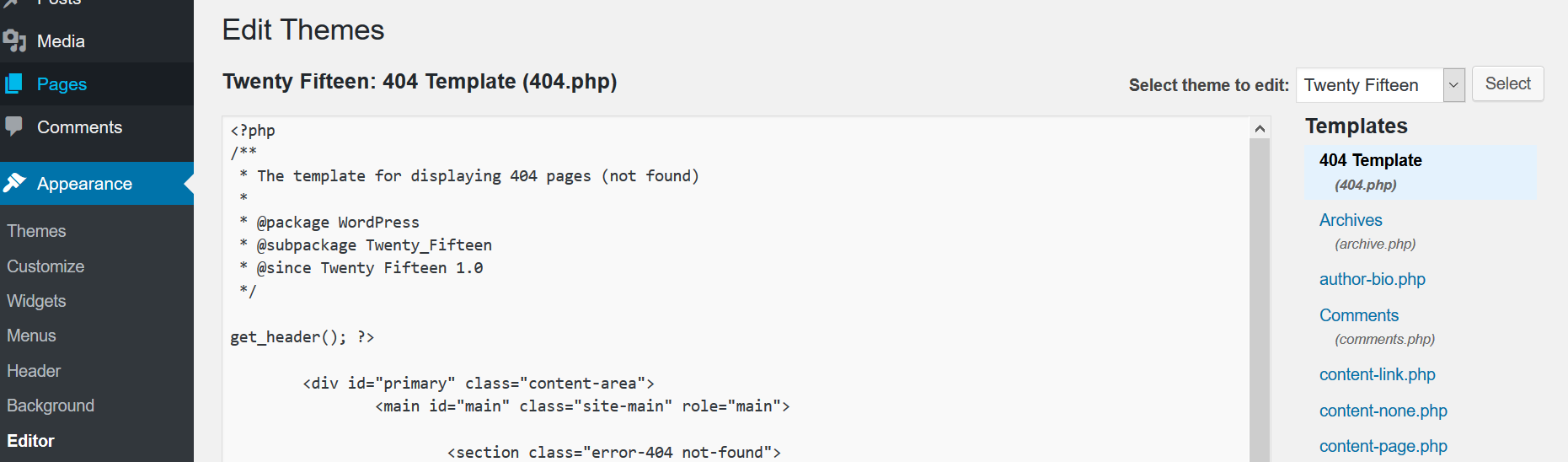


# 0x04:后台上传反弹shell

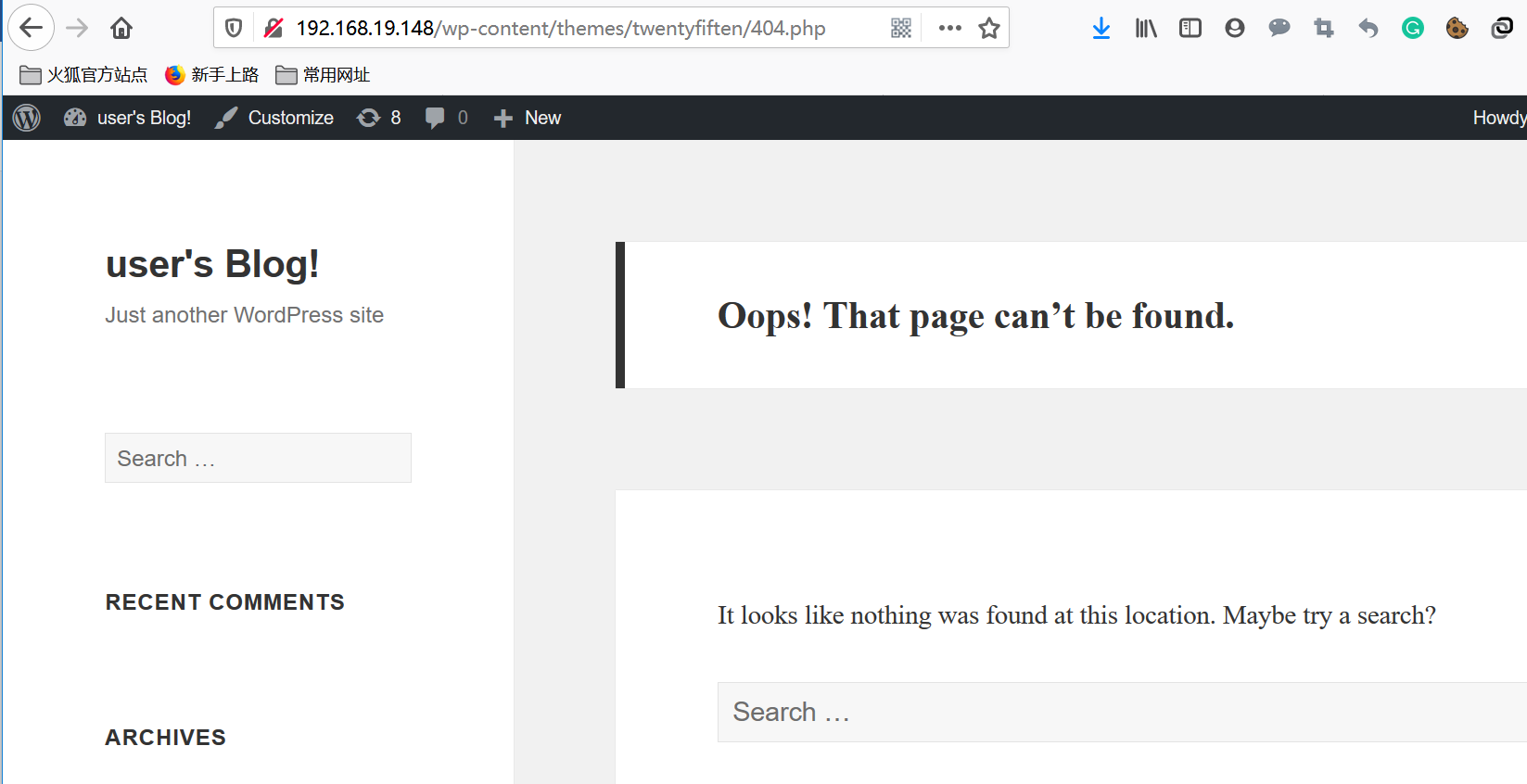
这里利用手中的账号Elliot ER28-0652登录一波去看了用户那里，目前应该是管理员身份



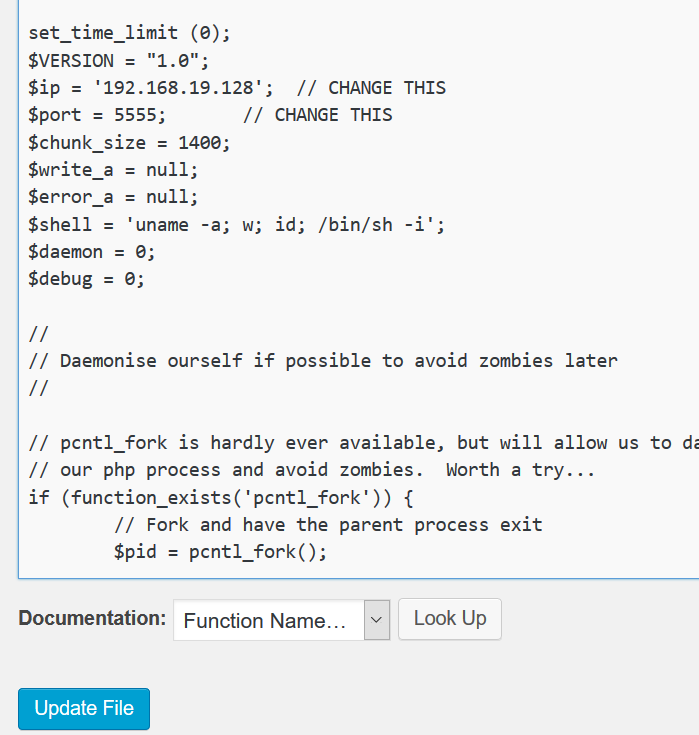
然后在Apperance/Editor/这里找到可以修改PHP源代码的地方那么可以在这里传一波反弹shell上去



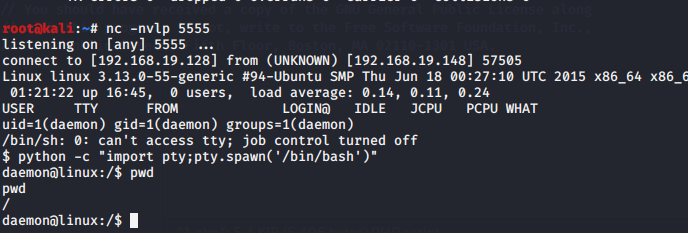
同时找到了前台的地址是<http://192.168.19.148/wp-content/themes/twentyfiften/404.php>



把反弹shell复制下来，改为kali的IP和端口

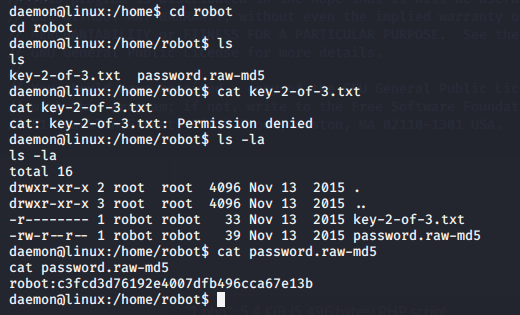


访问<http://192.168.19.148/wp-content/themes/twentyfiften/404.php> 记得提前开启nc就可以得到一个反弹shell了

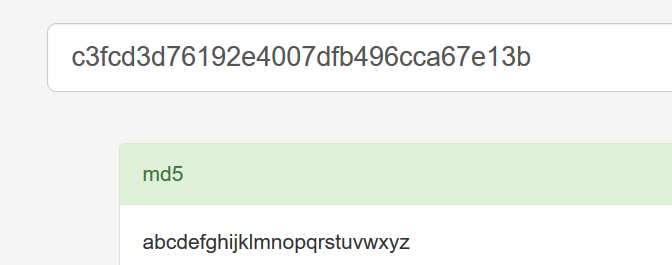


# 0x05:挖掘key

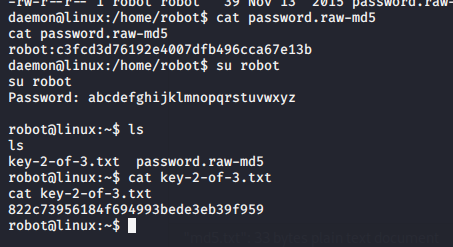
这里来到/home/robot目录下想读key结果发现没得权限，却可以读到password,里面有个账号和应该是MD5加密



这里拿去解密，密码有点。。。。。。

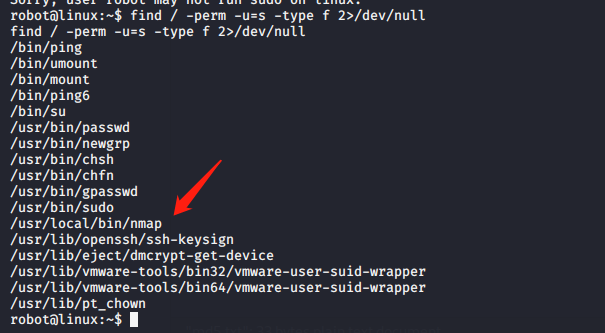


不过还是能成功得到第二个key

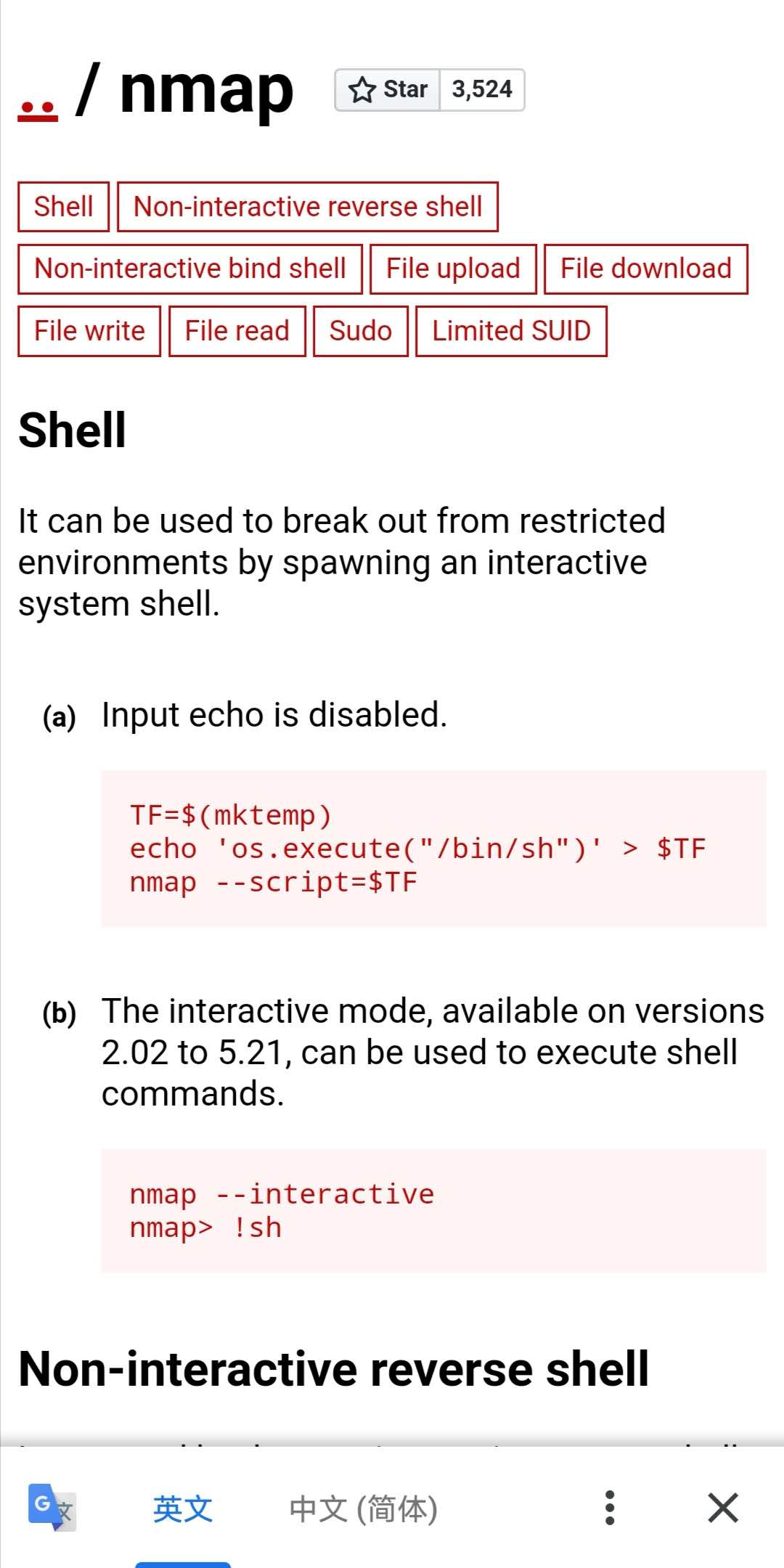


# 0x06:提权

这里我用find 找到了一个nmap(别问为什么不用sudo -l先，问就是没权限)



直接上去找了一下有提权方法



直接nmap –interactive 再来个!sh就可以变成root了，只不过不能一步CD到位

