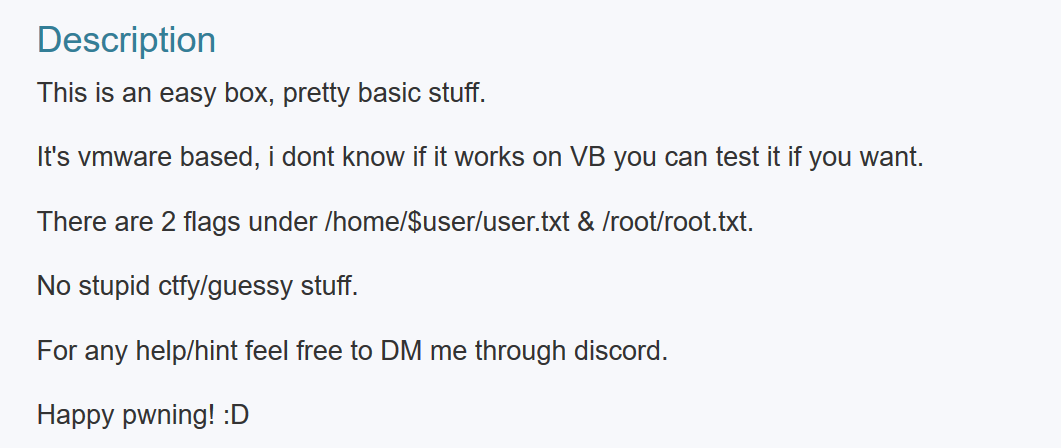
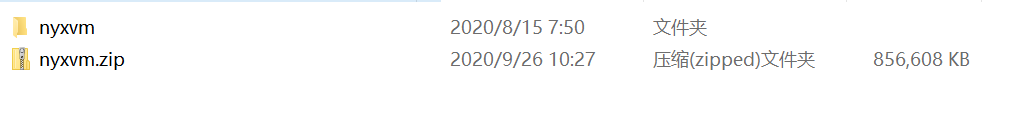
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/nyx-1,535/>

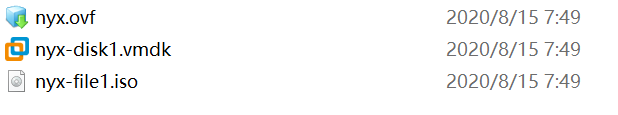
难度为简单，用VM安装，有2个flag



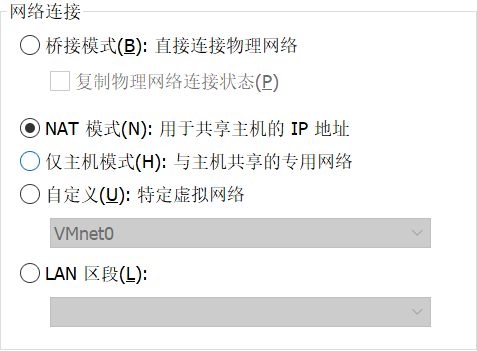
下载完以后解压有个文件夹



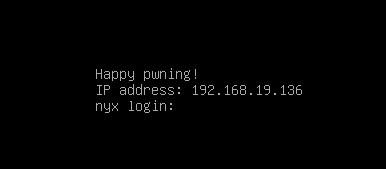
点进去以后有个.ovf文件双击点开找个地方存放就可以了



网络连接记得调回NAT模式



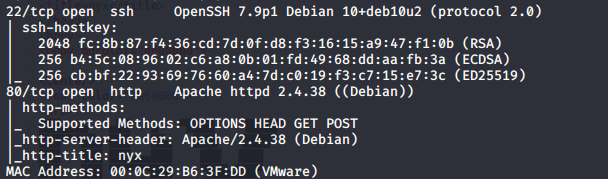
开机运行以后会自动回显IP出来



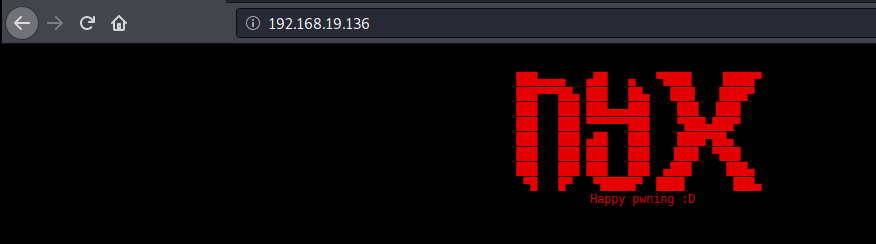
# 0x01:探测靶机

由于知道了IP直接用nmap探测波端口还是只开了22和80，2个端口

命令:nmap -A -sS -sV -v -p- 192.168.19.136

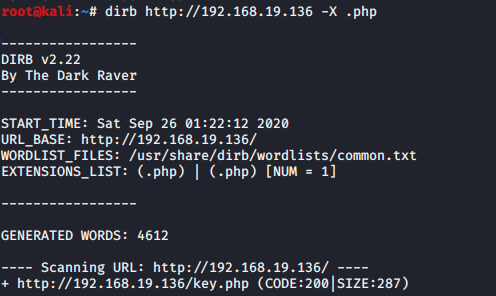


访问波IP可以正常回显，开搞

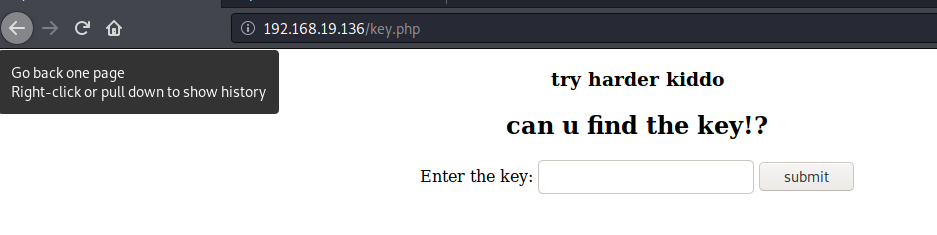


# 0x02:挖掘漏洞

先用dirb探探路正常加ip扫不出来，只能用扩展名扫出一个key.php的页面

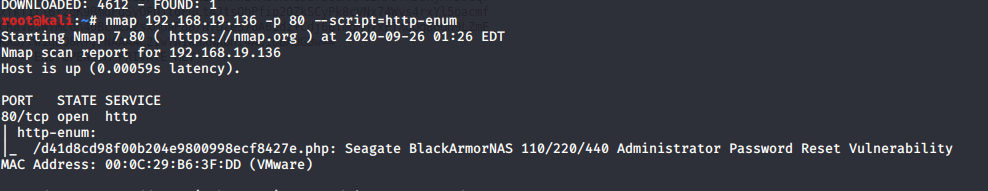


跟进以后是要提示找到key?逐渐感到迷惑

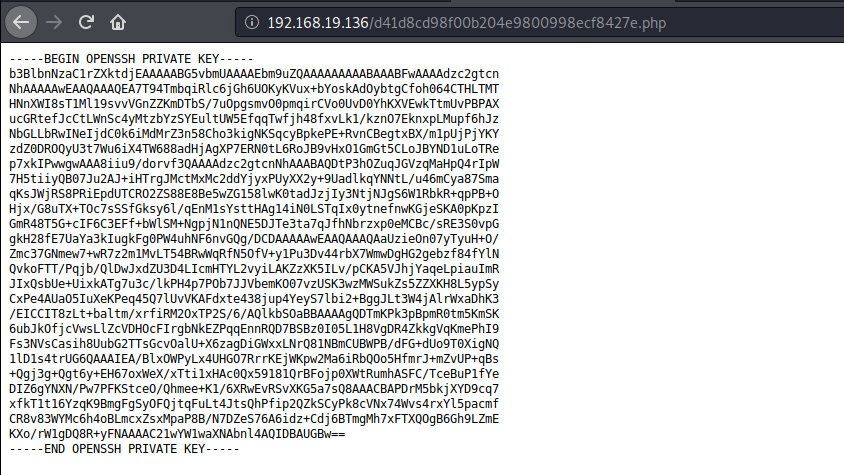


这个时候返回nmap，用另外一种方法就是script, nmap里面有很多script可以帮忙验证漏洞或者是帮忙枚举，这里选择的http-enum是用来从HTTP服务器上收集更多的信息，找到一个奇奇怪怪的php页面

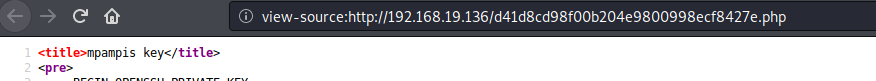
命令: nmap 192.168.19.136 -p 80 --script=http-enum



跟进以后发现中奖了，是SSH的钥匙

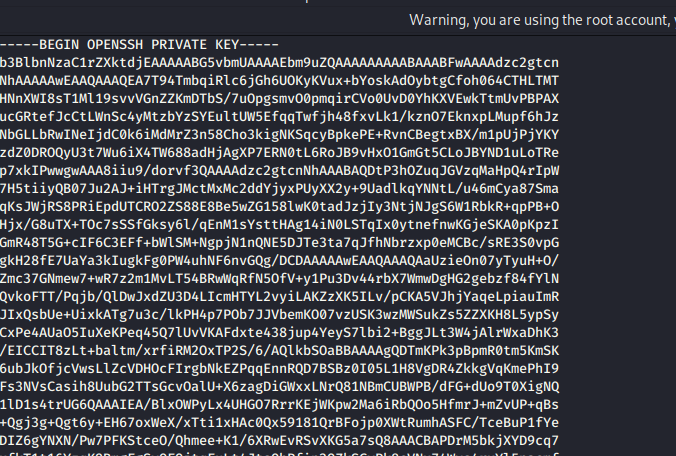


同时查看网页源代码从标题可以得知username可能就是mpampis

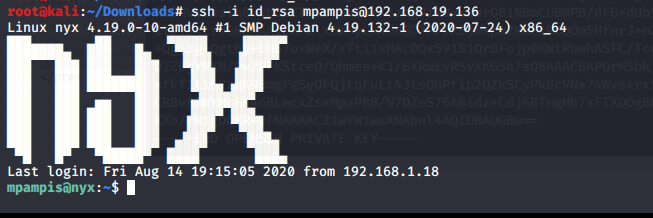


# 0x03:登录SSH端口

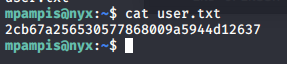
这里由于之前打其它的靶机创建过id\_rsa的文件了所以我就直接复制代替里面的旧内容了，权限也设置好了



直接ssh指定文件登录成功

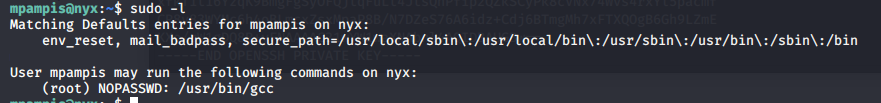


顺便得到第一个flag

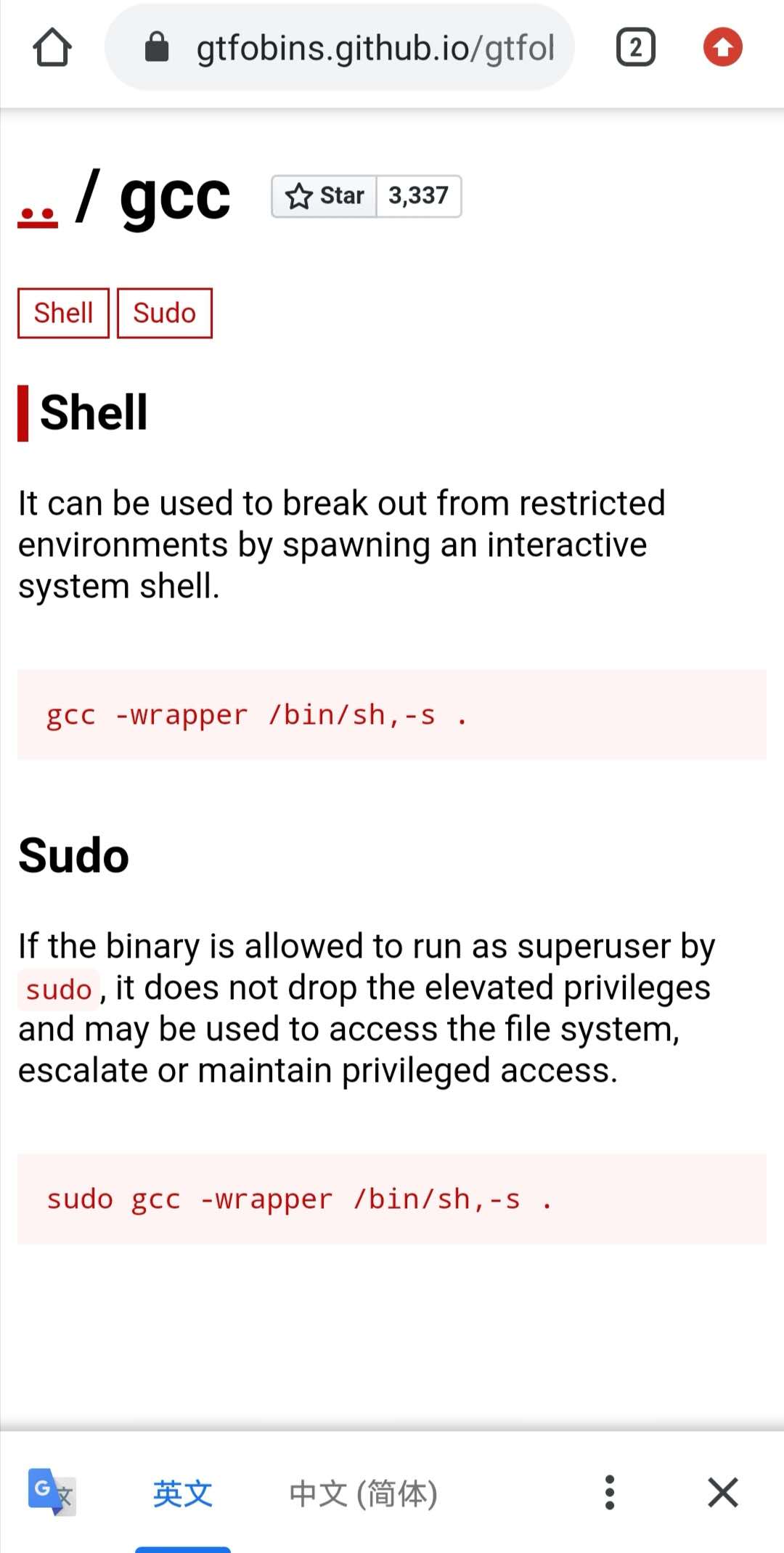


# 0x04:提权

Sudo -l这次也活下来了，只不过这次是gcc?????



经过多方查找找到这样一个方法



实践一波提权成功，提权那波属实有点懵逼大佬还是强的呀这也能提权

