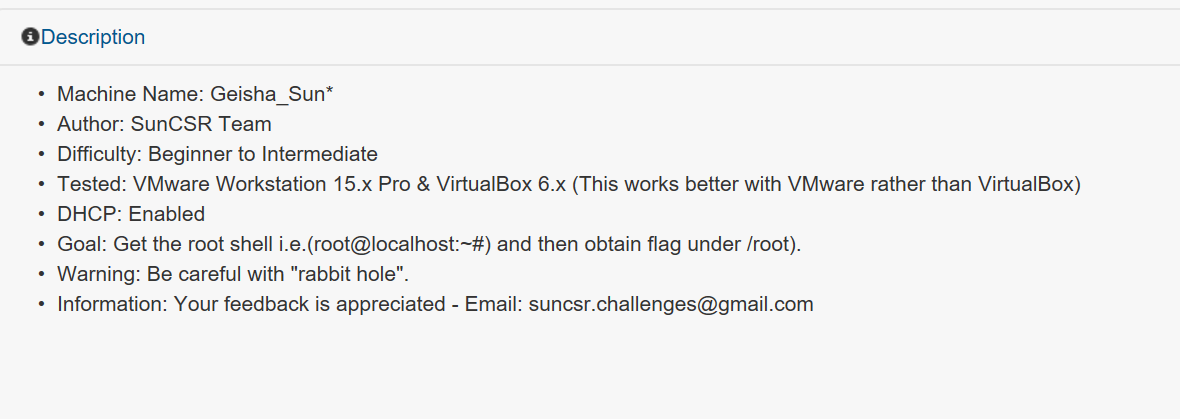
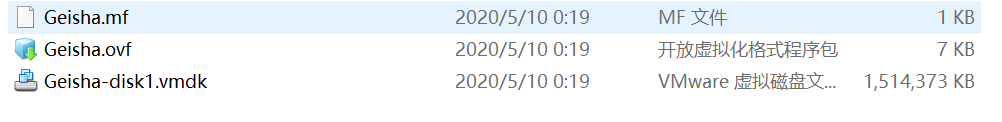
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/geisha-1,481/>

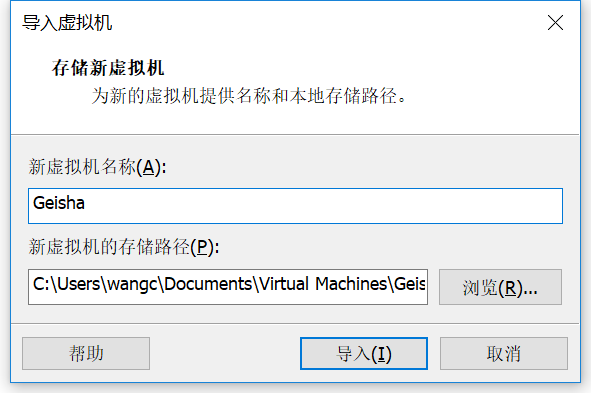


目标是拿到root权限

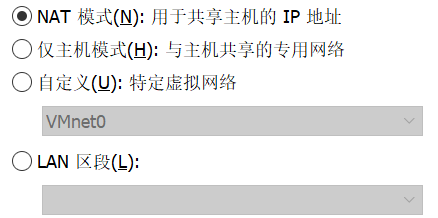
解压完以后可以看到这3个文件



点击Geisha.ovf会弹出导入虚拟机界面，选择一个新的空文件夹即可

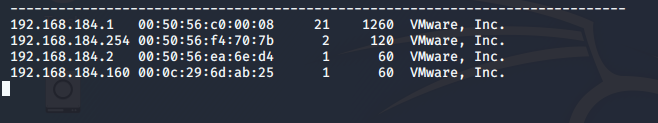


需要调回NAT模式，默认是桥接模式不一定有IP



# 0x01:探测靶机

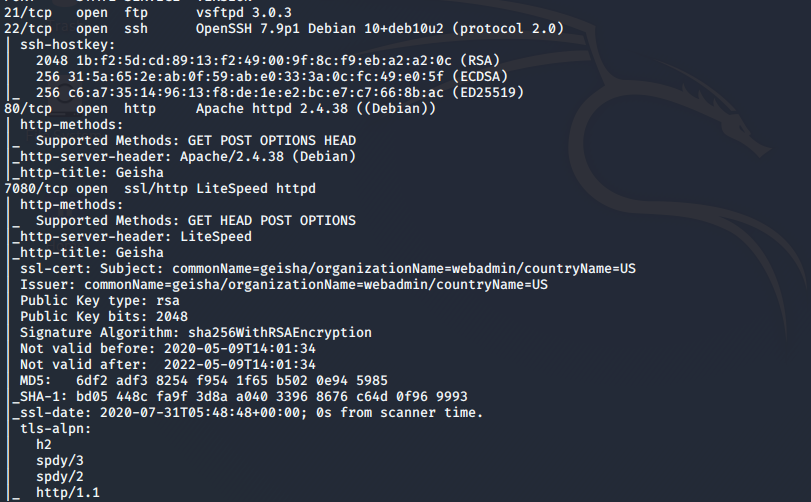
还是先用netdiscover探测靶机,排除.1,.254,2可以确认靶机为192.168.184.160

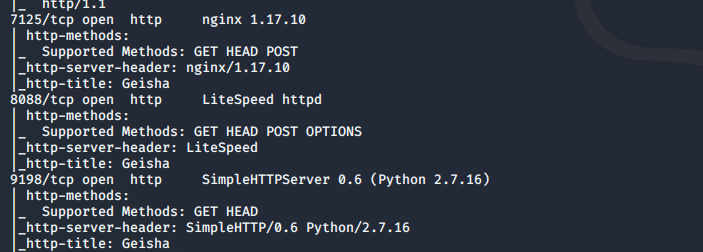


命令:netdiscover -r 192.168.184.0/16

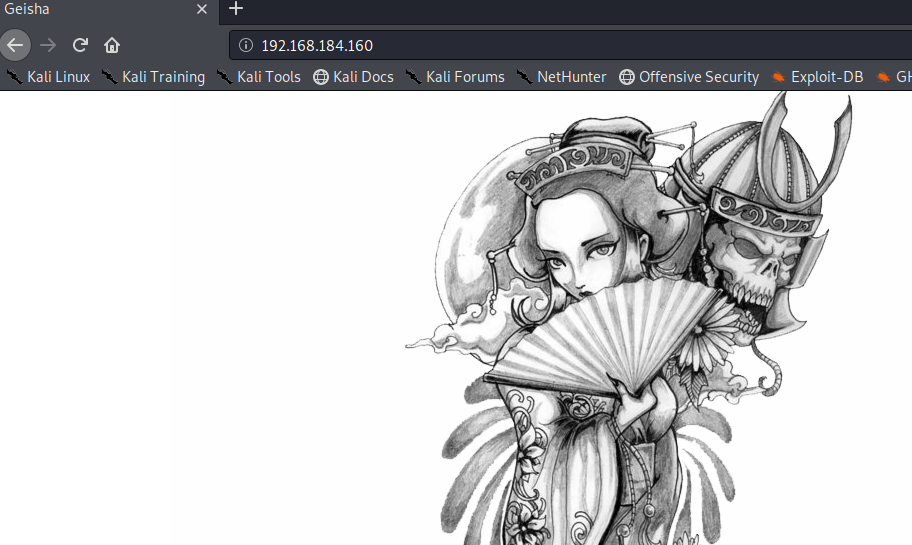
接下来就是用nmap探测端口，这次开放的比较多的端口,开了21，22，80，7080，7125，8088和9188端口

命令:nmap -A -sS -sV -v -p- 192.168.184.160





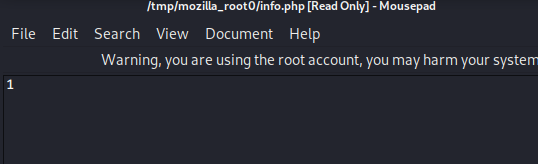
尝试的访问了一下各HTTP端口然而只有80是可以返回正常的，其它都不能连接



尝试用dirb进行目录扫描然而扫不出东西来

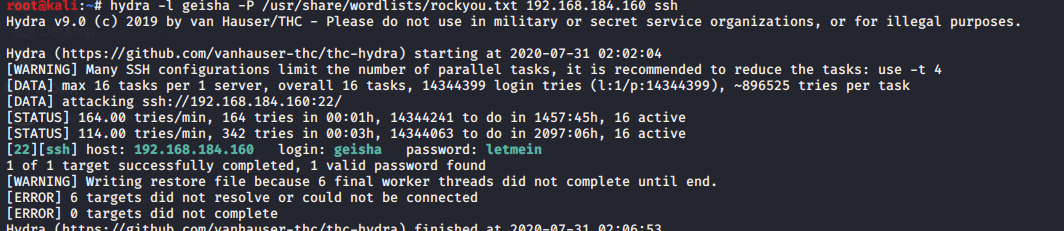


访问info.php只有1.。。。。。

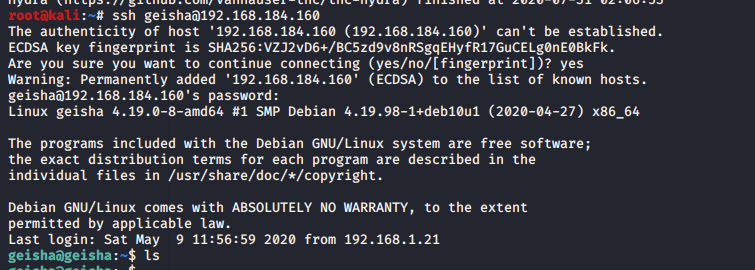


# 0x02:爆破22端口

这里只能把目标放回22端口，假设目标用户名为geisha,然后用kali的自带字典/usr/share/wordlists/rockyou.txt进行爆破最后能跑出一个用户名和密码出来



输入密码以后成功登录

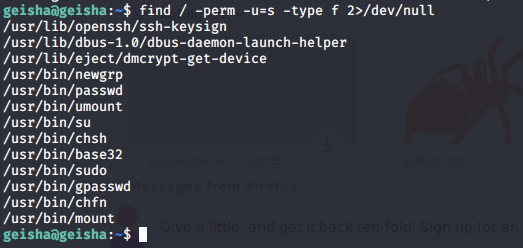


# 0x03:提权

先尝试一下用sudo -l，然而卒



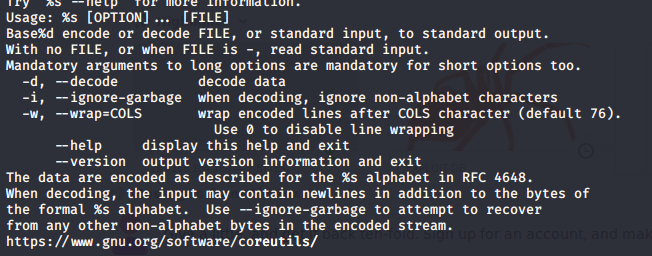
换成find / -perm -u=s -type f 2>/dev/null查找SUID权限, 发现一个奇怪的东西base32



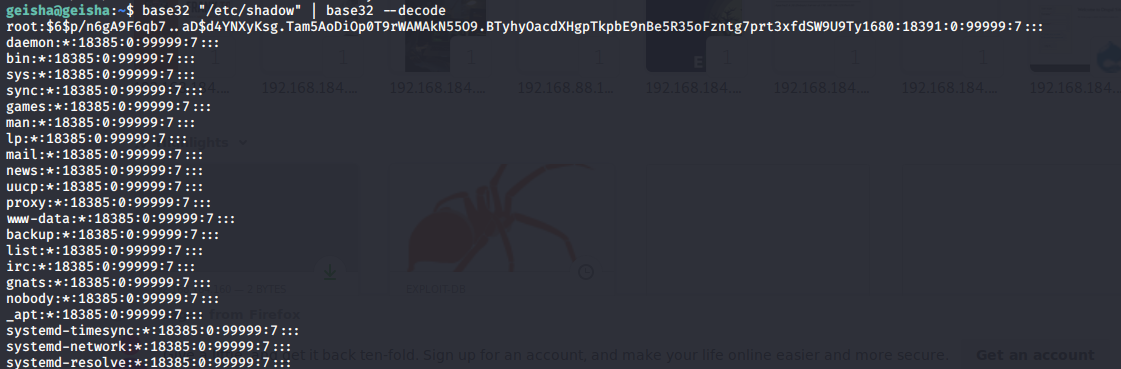
Ls了一下是个有点奇怪的root权限二进制文件



用strings /usr/bin/base32以后可以正常回显，顺便看到使用说明



Base32和base64其实也是一种编码只不过base32要比base64功能上弱一点，这里有个想法linux密码会存放在/etc/shadow里面，尝试用base32， 看到有root的值，用john破解失败



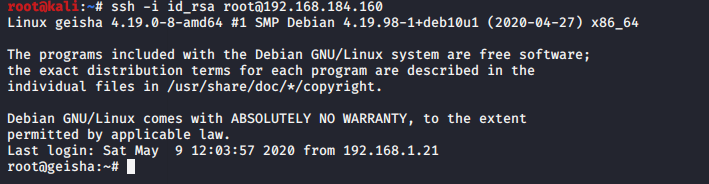
这里还有一个想法复制一波root目录下的ssh文件然后无密码的状态上登录进去，复制下来保存到本地



一定要给权限



然后用ssh连接成功



最后获得flag

