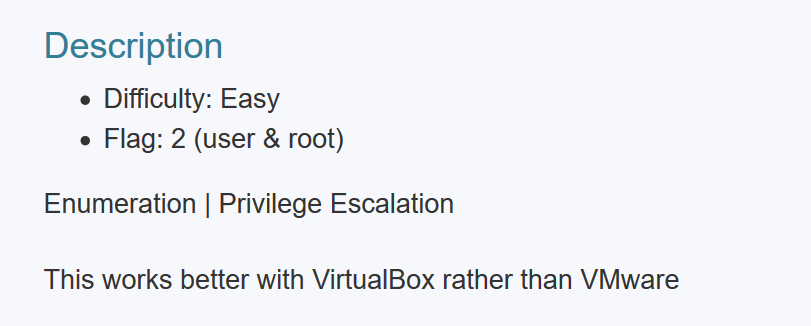
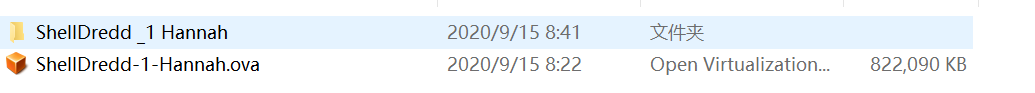
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/onsystem-shelldredd-1-hannah,545/>

难度简单，有2个flag，主要目的是枚举和提权，建议在VirtualBox下进行搞破坏



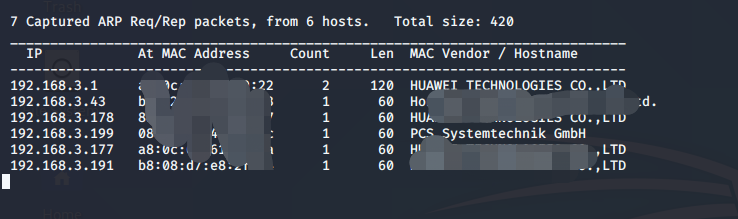
由于是virtualbox直接导入就好了，网络为桥接网卡



# 0x01:靶机探测

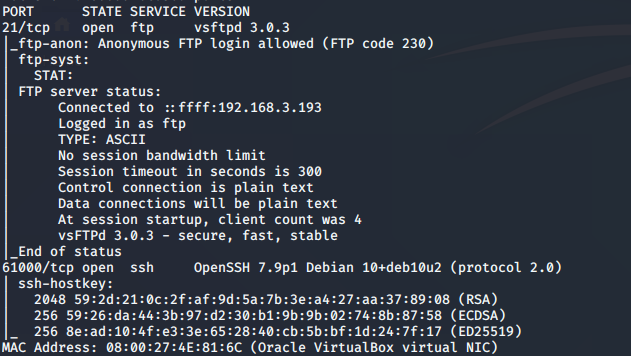
还是先用Netdiscover探测一波，直接找PCS,可以确认靶机IP为192.168.3.199

命令:netdiscover -r 192.168.3.0/16



开始用nmap探测端口,只开了21和61000两个端口，没HTTP服务。。。。顺便21端口支持Anonymous访问

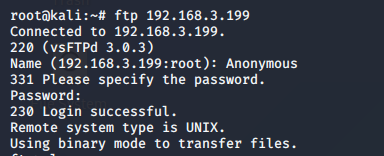
命令:nmap -A -sS -sV -v -p- 192.168.3.199



# 0x02:挖掘信息

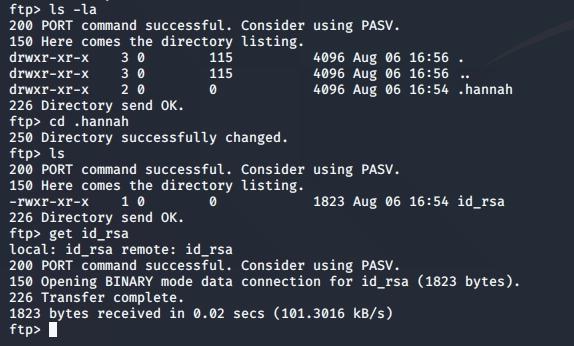
由于没HTTP服务这里就不访问IP了，直接访问21端口，成功登录

命令:ftp 192.168.3.199 用户名为Anonymous 密码:无

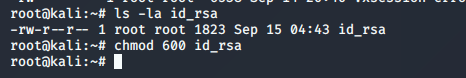


然后就用Ls列出当前文件目录为防止丢失隐藏文件用ls -la结果发现一个.hannah的隐藏文件夹，跟进以后得到一个id\_rsa。然后下载下来。

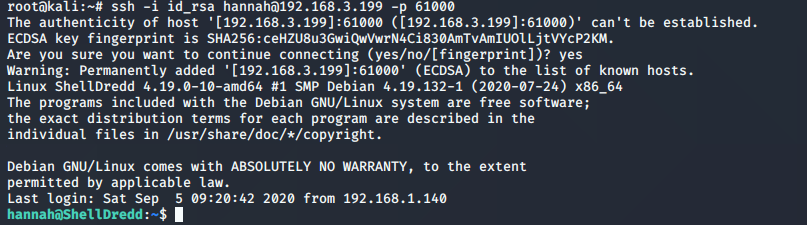
(id\_rsa可以理解为SSH登录通行证，想要登录其它机器的SSH端口要嘛输入账号密码或者是用id\_rsa刷卡进入这样理解)



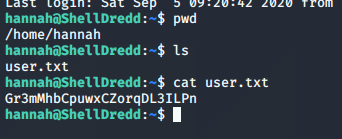
下载完以后要记得给权限才能运行



然后用SSH连接成功(用户名纯属硬猜，因为靶机名字到文件夹都是hannah)。

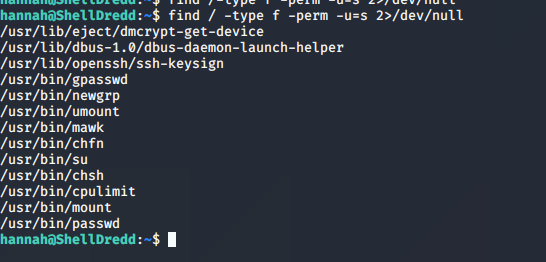


得到第一个flag,user的



# 0x03:提权

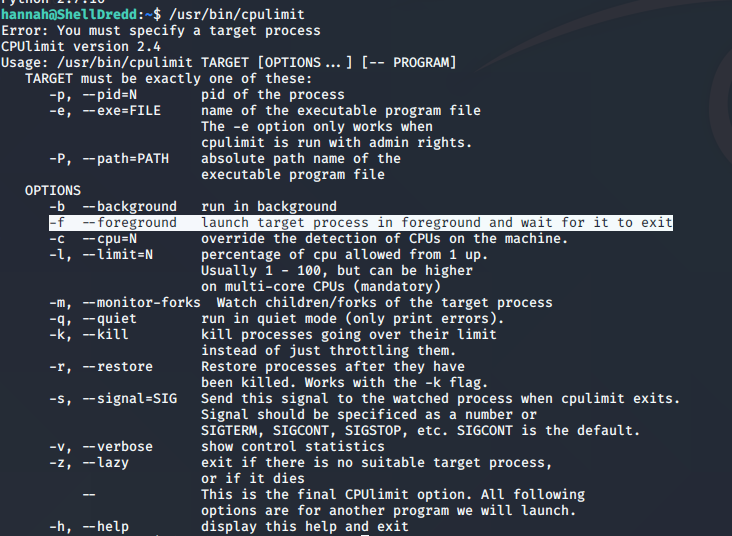
Sudo -l日常暴毙，只能换另外一个找到有个特别的东西cpulimit



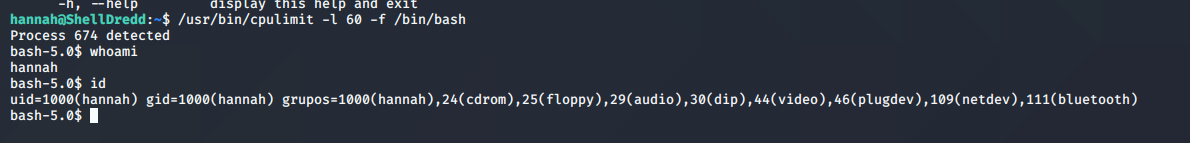
查看了一下很明显是一个二进制的文件



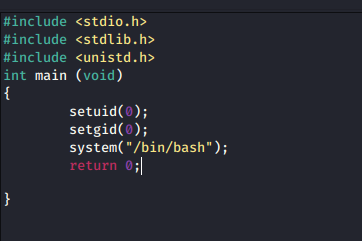
还可以看到使用说明



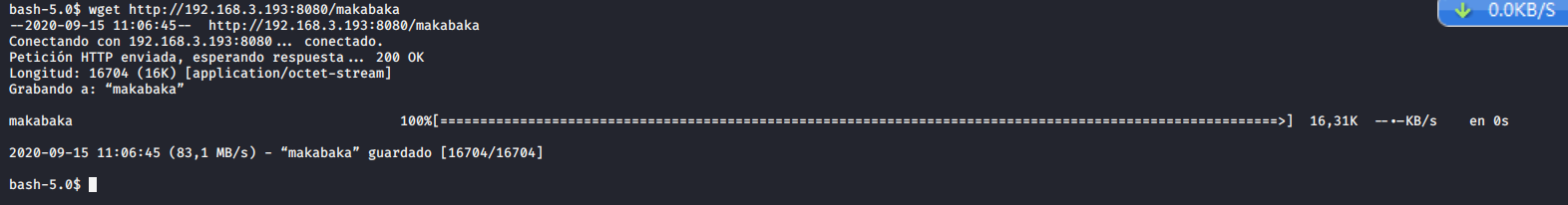
运行了一波，似乎可以帮你设置SUID，但是对提权命令无效不知道为啥。。。。。



由于-f 是可以对一个文件的，所以可以自己写一个出来，比较简陋，然后用gcc编译一下传上去



然后在目标服务器上下载下来



运行前记得给权限然后直接运行就可以得到root权限

