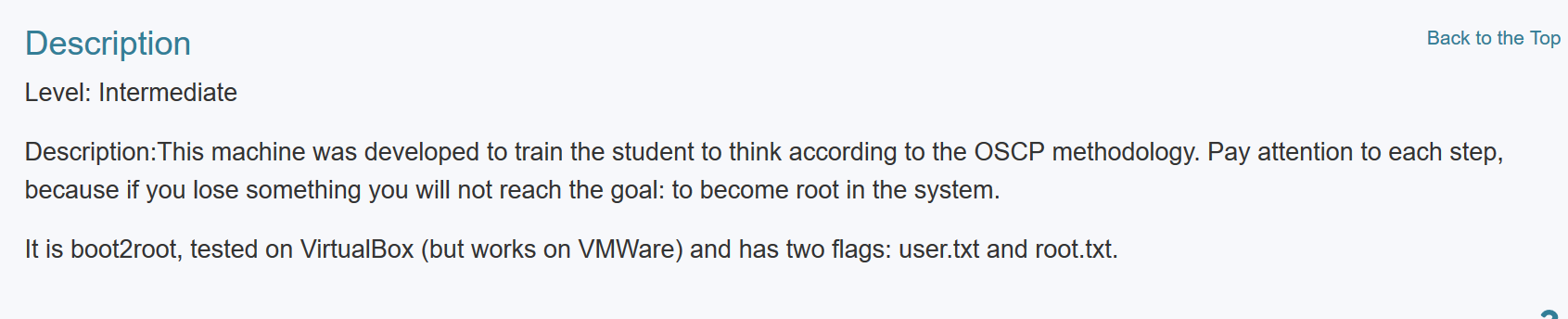
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/healthcare-1,522/>

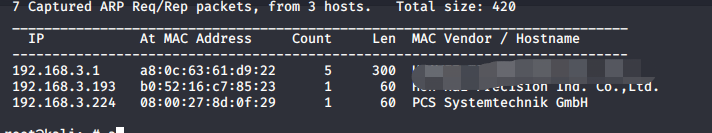
难度为中等，这个靶机是给想考oscp准备的，注意每一步，否则很难拿到root权限，在virtualbox下进行有2个flag



# 0x01:探测靶机

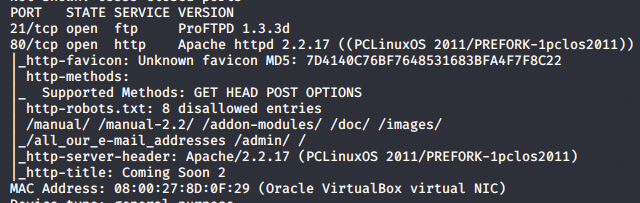
由于是virtualbox就偷懒写安装方法了。还是先用Netdiscover这里调来调去终于把IP给正常调回来了这次终于只有一个PCS了，可以确定靶机IP为192.168.3.224

命令:netdiscover -r 192.168.3.0/16

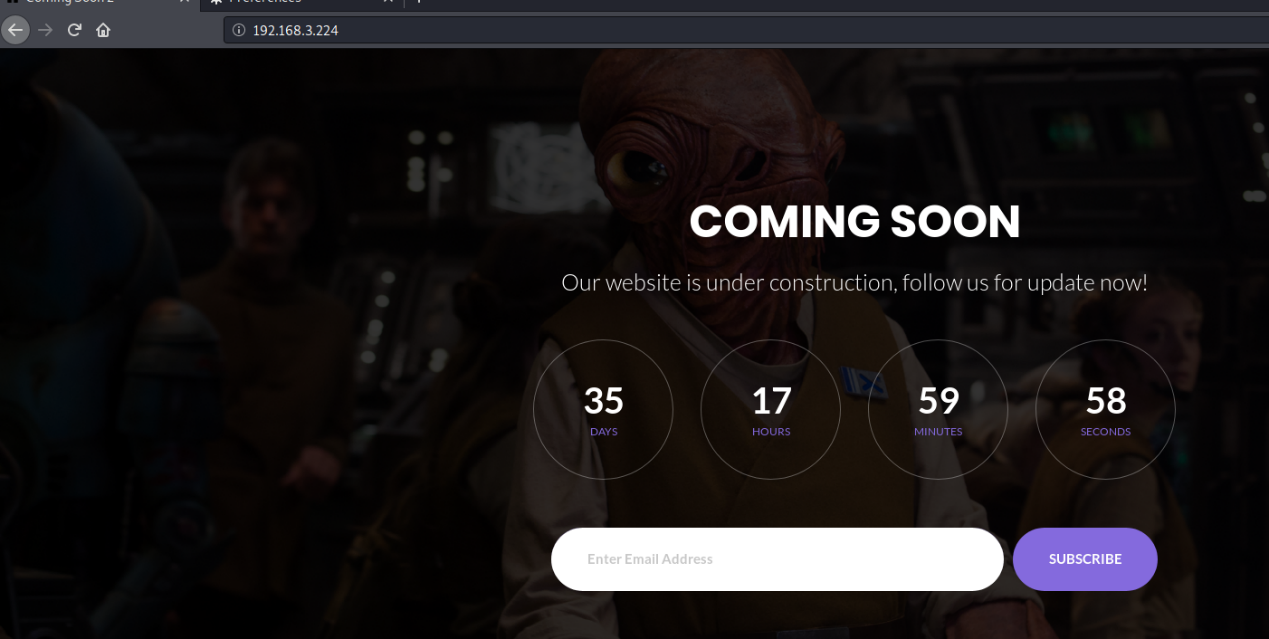


然后开始用nmap探测波端口,这次只开了21和80由于21端口没有显示可以匿名登录那就只能把注意力集中在80端口了

命令:nmap -A -sS -sV -v -p- 192.168.3.224

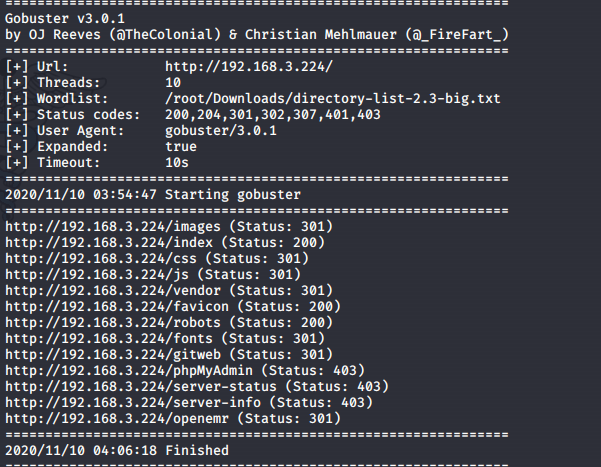


访问IP可以正常回显开挖

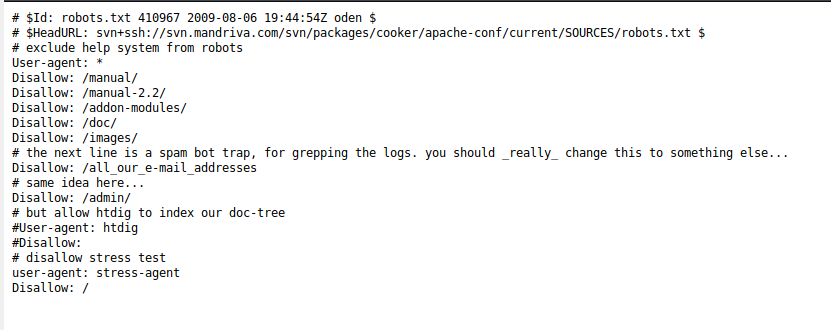


# 0x02:挖掘目录

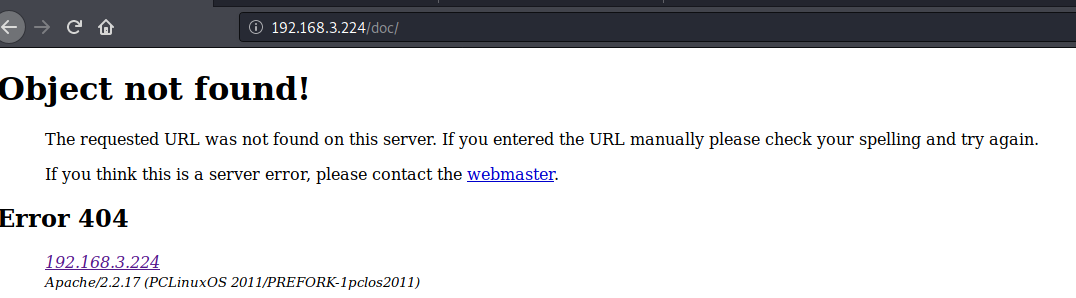
这里启用gobuster开始目录挖掘配大字典，可以挖到很多东西，不过先忽略4字开头通常是访问不了的



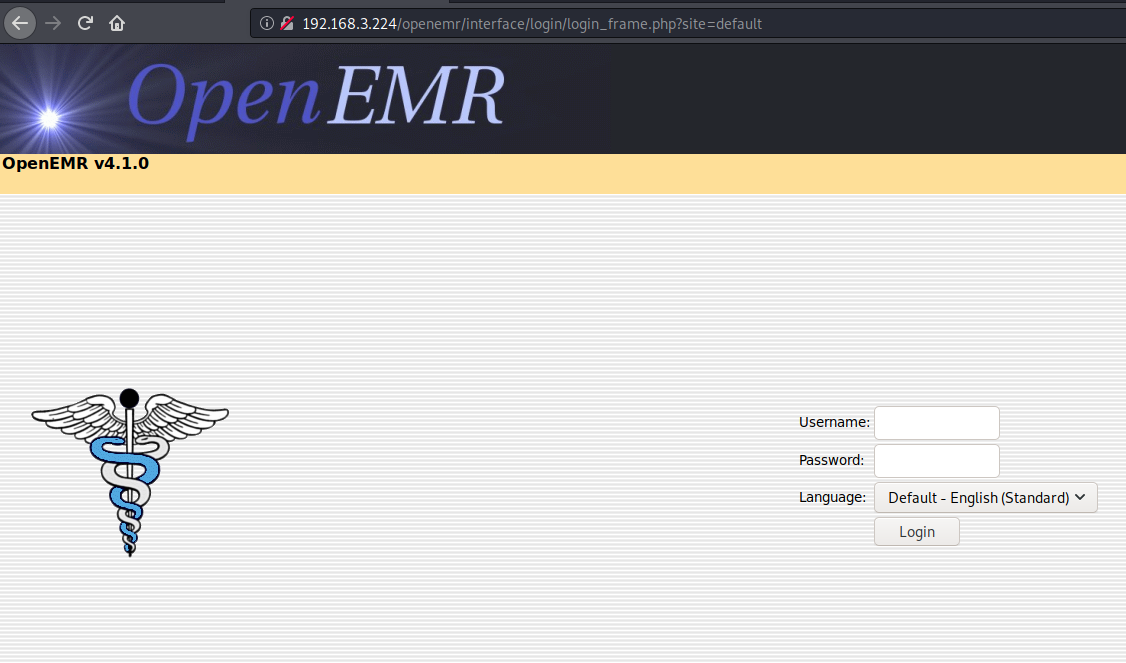
那就先跟进/robots.txt发现有很多隐藏的东西



然而跟进以后才发现全都访问不了，或者没权限

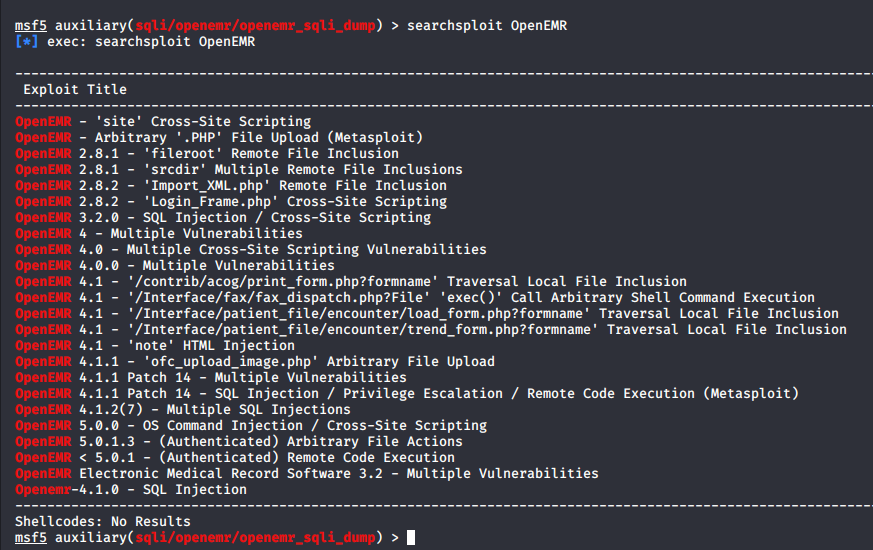


然后只能回到gobuster继续找其它链接，来到openEMR的时候哦吼CMS登录界面

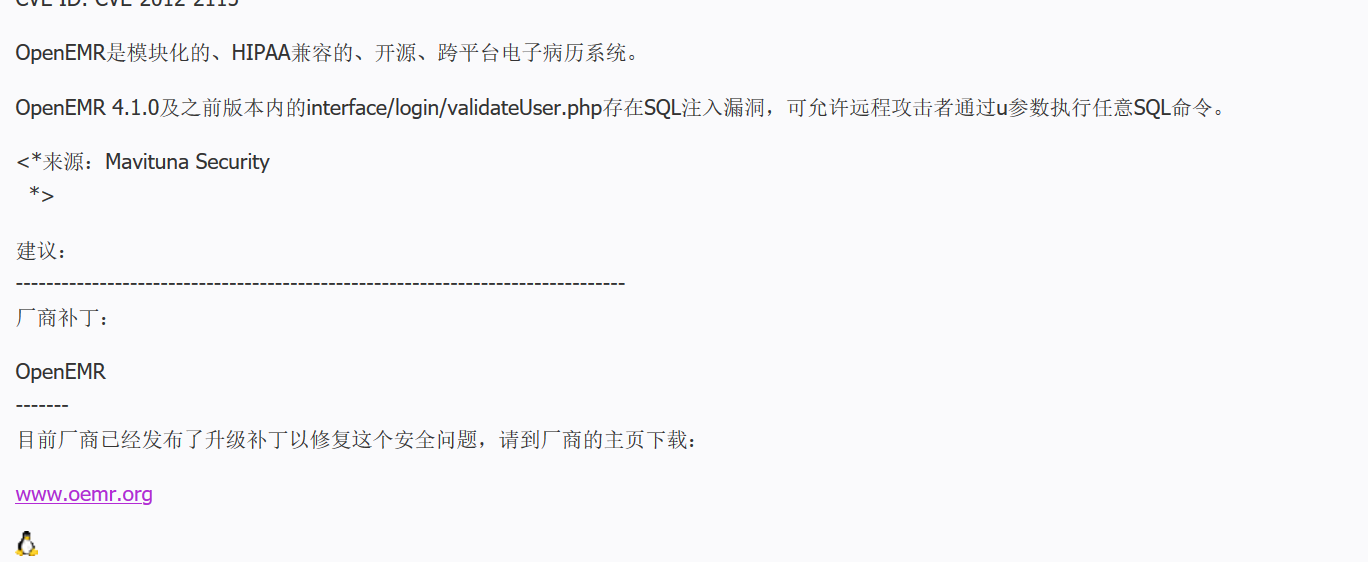


# 0x03:挖掘CMS漏洞

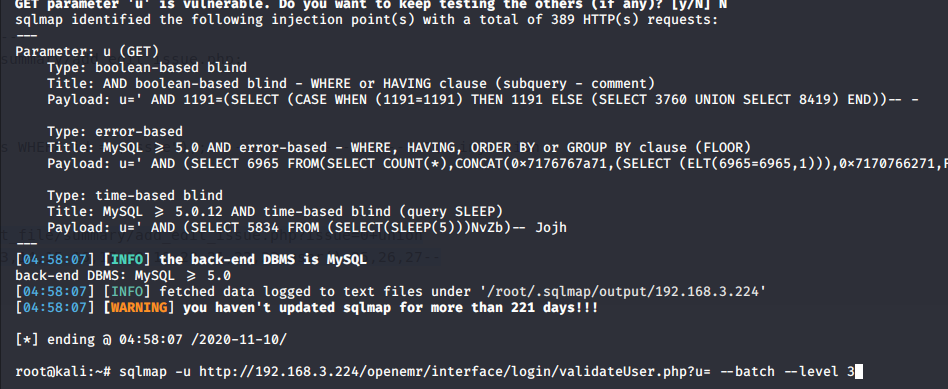
这里提取波关键词OpenEMR ,在MSF里面可以找到很多漏洞



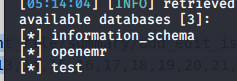
这里百度了以下有相关漏洞<https://www.linuxidc.com/linux/2012-09/70873.htm>



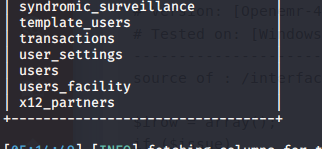
尝试用sqlmap确实存在漏洞



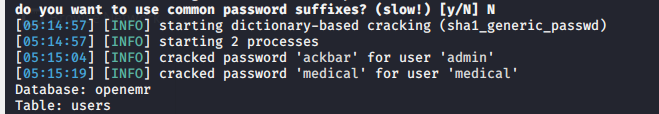
开始跑数据库，果断选择openemr



然后跑表里面的内容，由于表的数据太多了，只能挑关键词，找到一个Users表

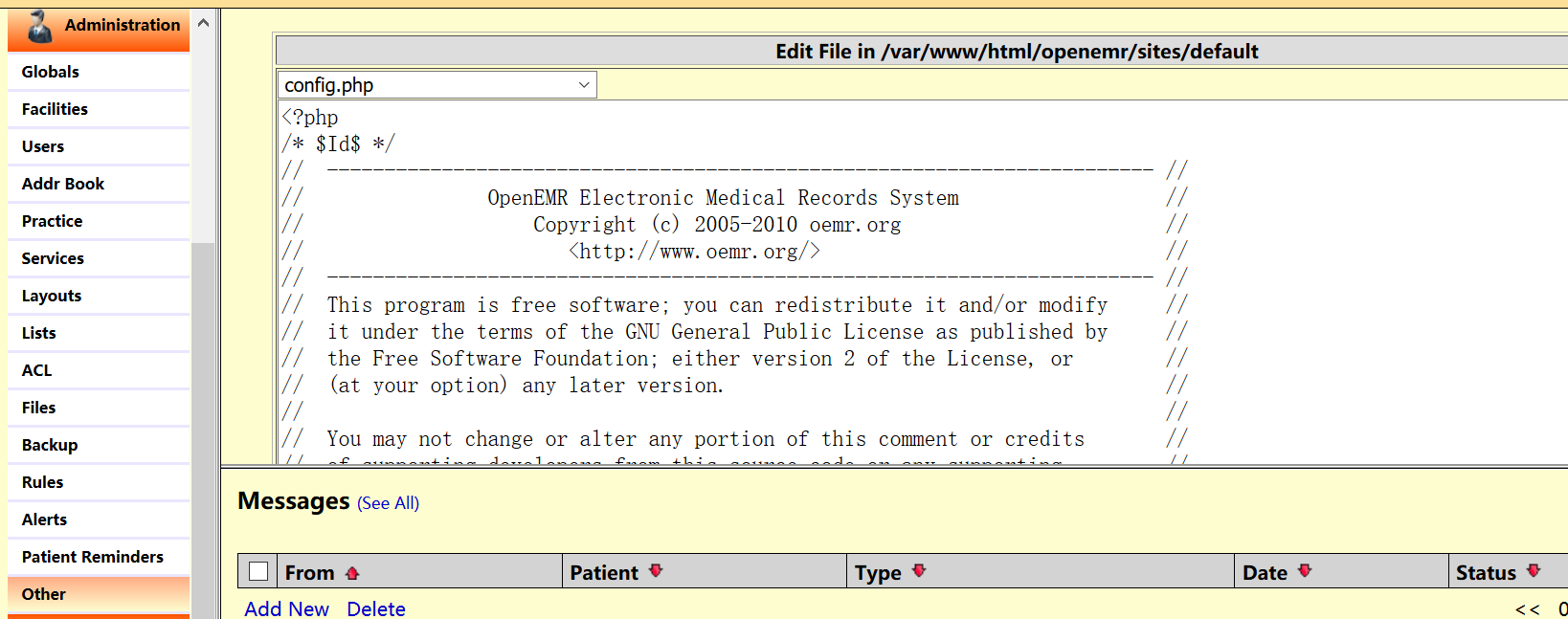


开始跑里面的数据，得到2个账户密码

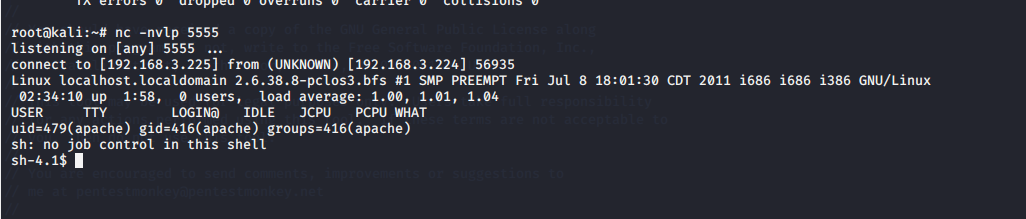


# 0x04:上传反弹shell

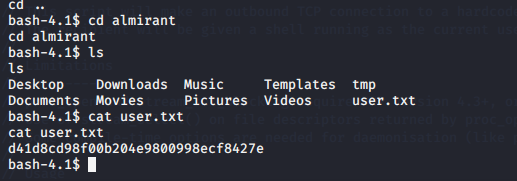
原本是想用MSF直接拿shell的结果上传出问题了，只能用admin账号手动登录，然后在Administration->Files->config.php这样找到可以编辑代码的地方，果断把反弹shell复制粘贴上去



然后在前台访问<http://192.168.3.224/openemr/sites/default/config.php>，记得提前开启nc就可以得到一个反弹shell了

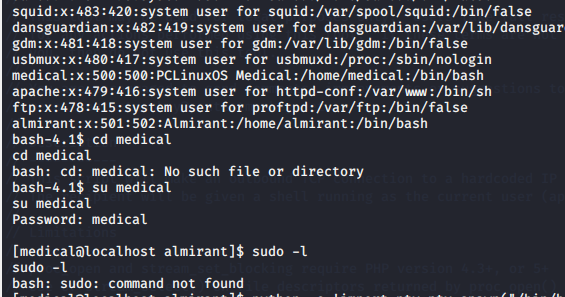


然后在/home/almirant得到user的flag

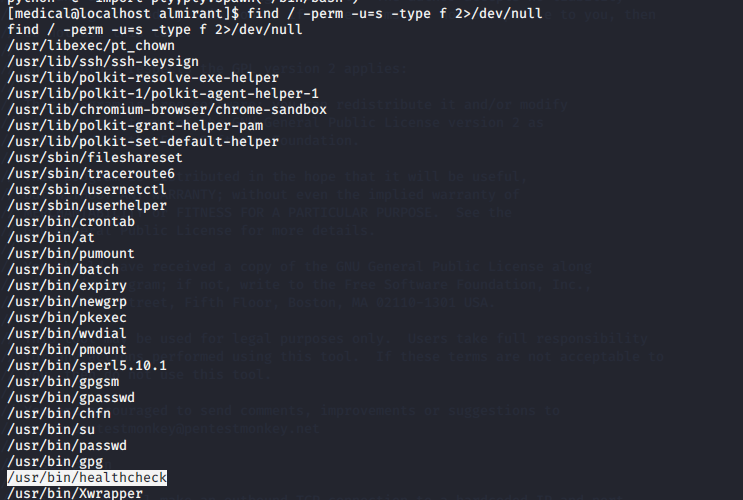


# 0x05:提权

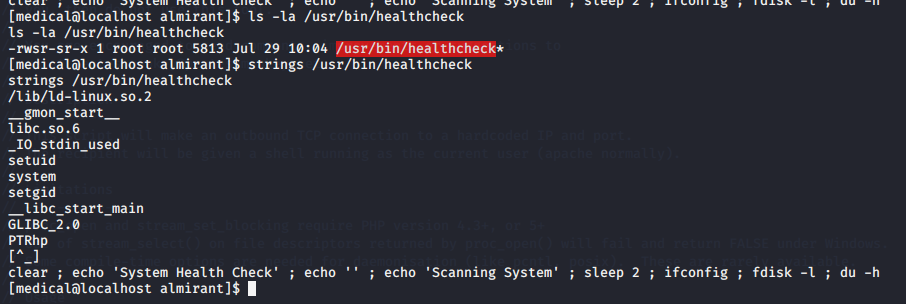
这里在用cat /etc/passwd的时候发现有个Medical用户，果断切换一波，然而sudo -l还是倒了



这里用find找到一个/usr/bin/healthcheck的程序



先用ls -la查看了一波是个二进制程序，只能用strings查看里面的内容，发现点东西,ifconfig(查看本地IP信息) ,fdisk -l(查看硬盘及分区信息) du-h(显示文件或目录大小)



也就是说可以尝试用echo打些命令执行漏洞进去比如/bin/bash进去，然而并不是。。。这里眼看着社团时间结束，大佬关上电脑走人赶紧上去保住大腿问了一波emmmm被大佬指指点点一波以后变成root了。。。但是有点懵逼

