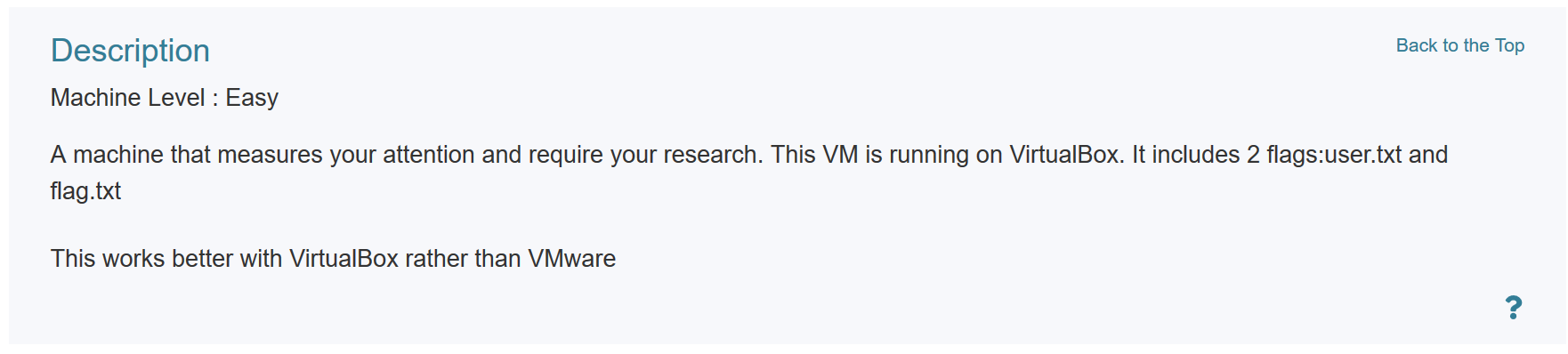
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/kb-vuln-2,562/>

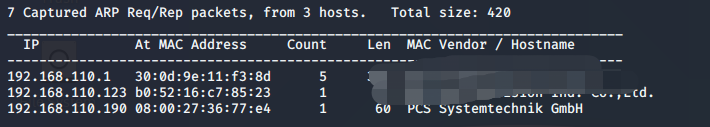
简单级别靶机。建议用VirtualBox来做包括两个flag一个是user.txt另外一个是flag.txt



# 0x01:探测靶机

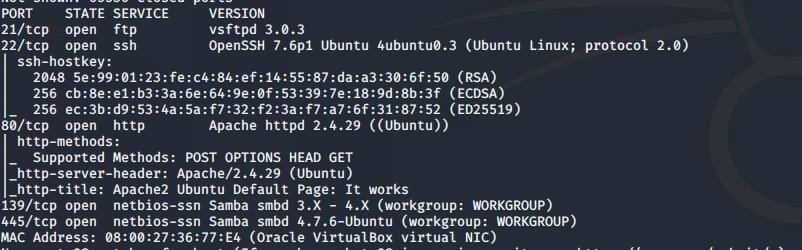
先用netdiscover探测波靶机,直接找PCS，可以确定靶机IP为192.168.110.190

命令:netdiscover -r 192.168.110.0/16

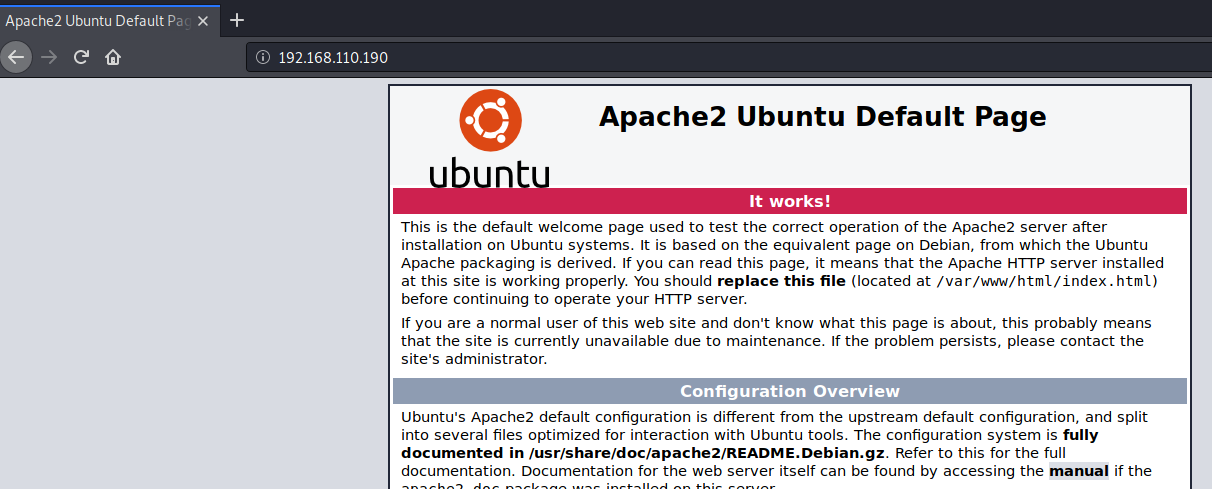


然后开始用nmap开始探测波端口,开的端口还比较多有21，22，80，139和445端口

命令:nmap -A -sS -sV -v -p- 192.168.110.190



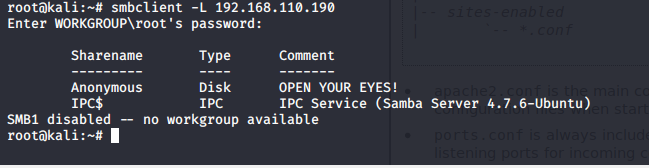
页面返回正常，开始渗透



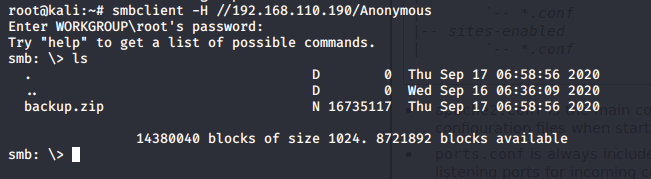
# 0x02:挖掘信息

由于知道开启了139和445端口可以用smbclient探查波信息,可以知道Anonymous可以用来登录一波密码默认为空，如果不是空放弃

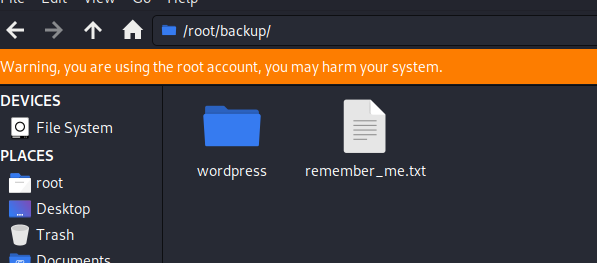
命令:smbclient -L 192.168.110.190 (-L可以理解为列出host出来)



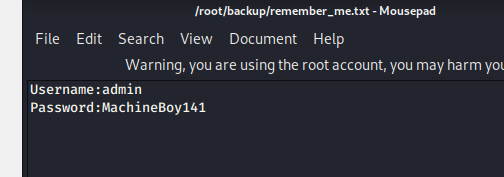
然后连接一波输入空密码以后成功登录发现一个backup.zip,用get +文件名下到kali



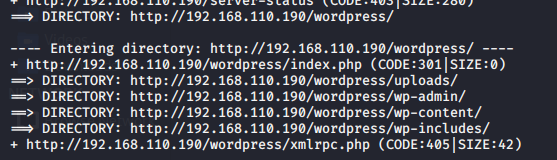
解压以后得到这两个文件，其中wordpress里面是详细的源码，这个靶机可能有wordpress站点



点开remember\_me.txt以后得到一个账号密码

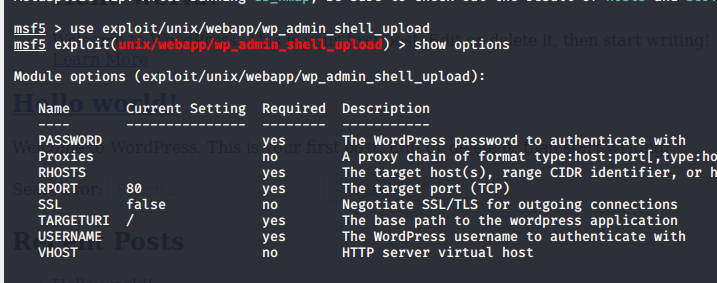


为了验证是不是wordpress站点用dirb探探路，扫到了



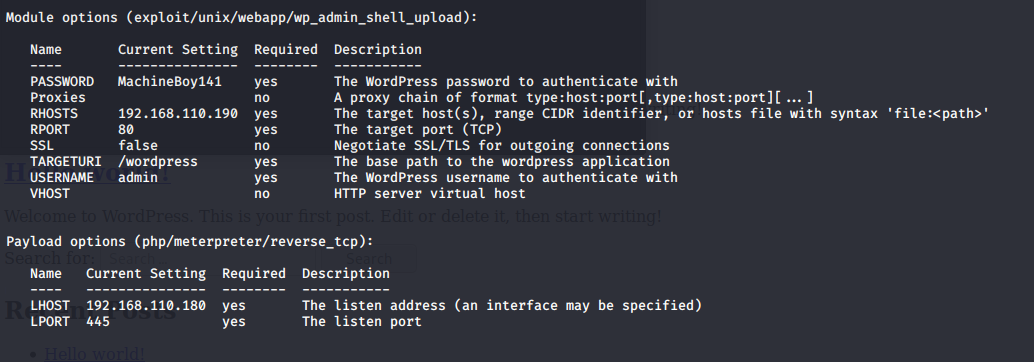
# 0x03:利用MSF getshell

由于目前知道了wordpress的管理员账号密码，以及wordpress路径可以用MSF 的exploit/unix/webapp/wp\_admin\_shell\_upload来gets hell一波

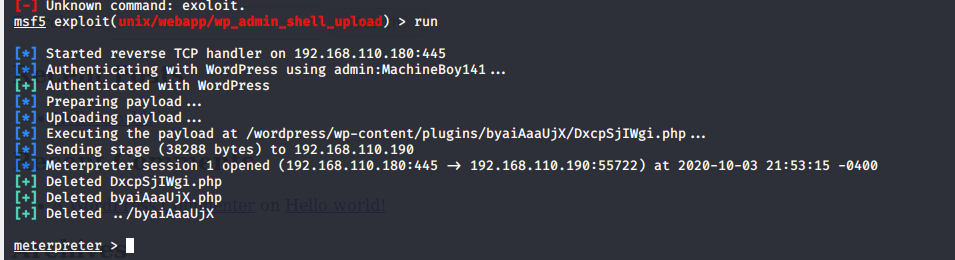


设置波参数,最后的效果图，为什么lport得445呢?我也不知道因为我设置默认端口不行，139不行，500不行，5000不行，3000不行，445行。这也让我有点迷惑

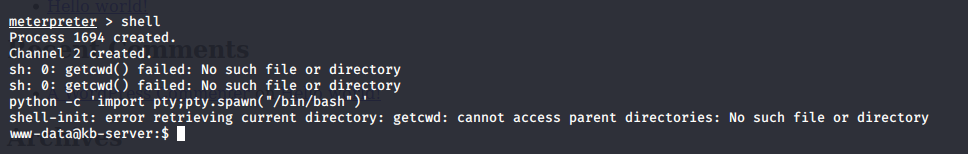
命令:set RHOSTS 192.168.110.190 set USERNAME admin set PASSWORD MachineBoy141 set TARGETURI /wordpress set lport=445



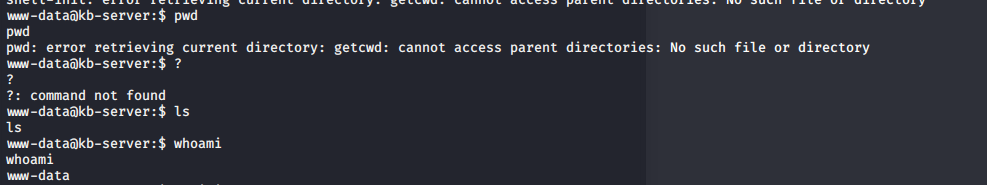
输入run以后出现meterpreter就是代表成功了



然后输入shell在打一条python的交互shell进去

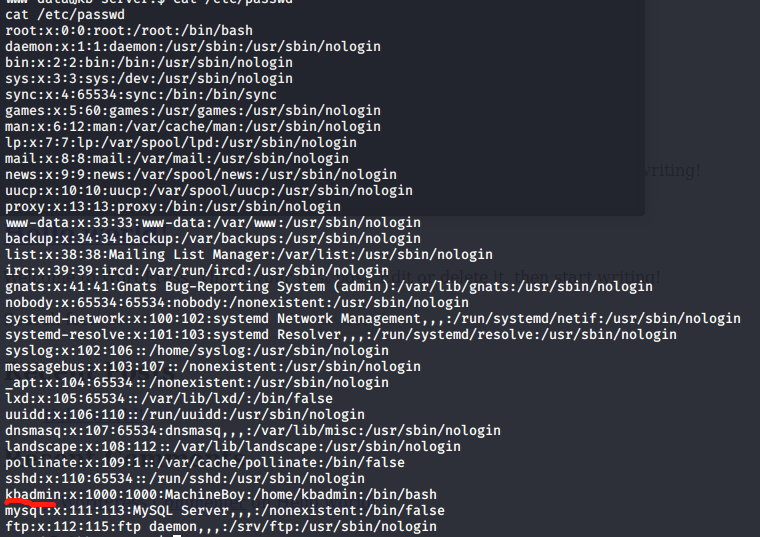


不过好像是个有限制的shell

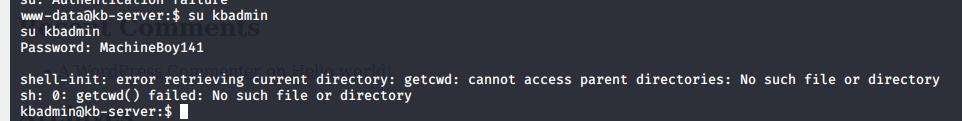


# 0x04:切换用户

先看一波用户名看到有个kbadmin，跟admin好像

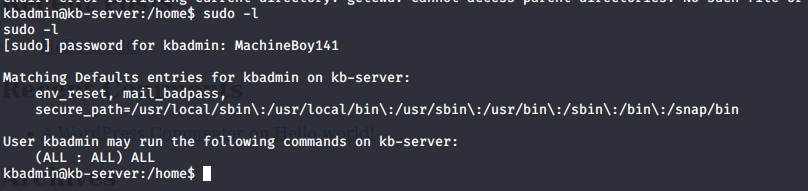


切换一波输入空密码错误，输入跟admin一样的密码成功了。。。。。



# 0x05:提权

输入一波sudo -l,又遇到输入密码我以为会告诉我没得特殊权限结果权限那么大



直接一波sudo su root切换成功，只不过好像是要用docker提权的。。。。好吧，直接读到flag了

