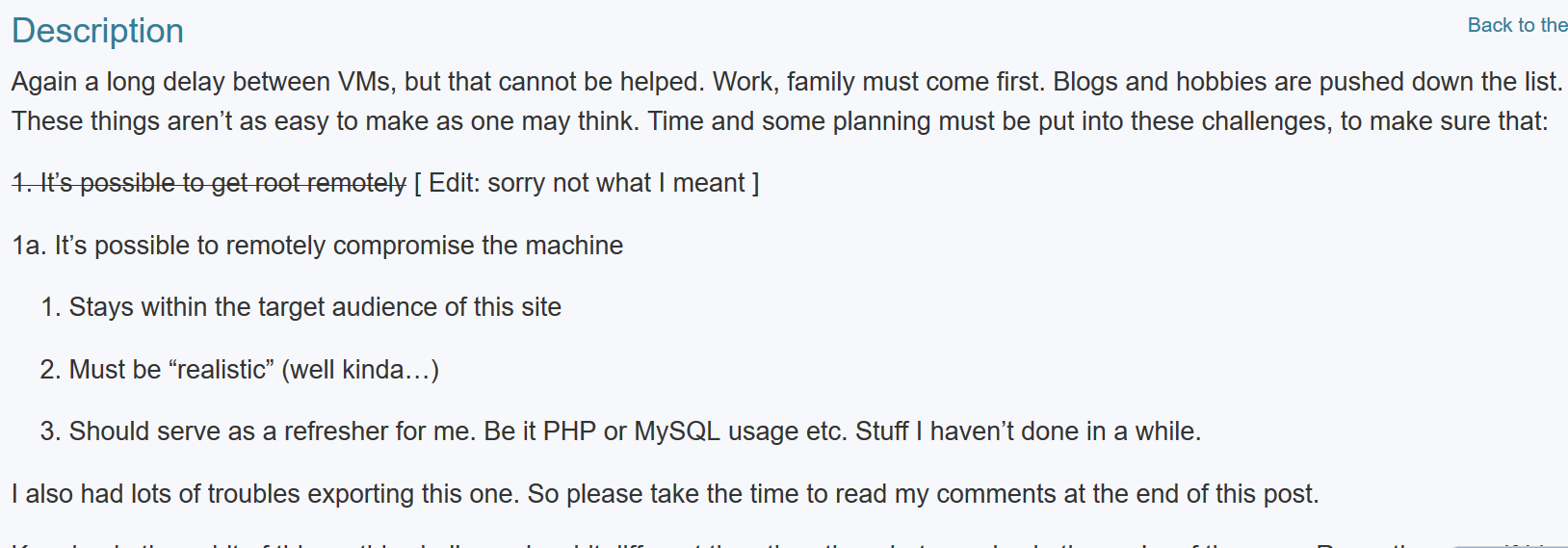
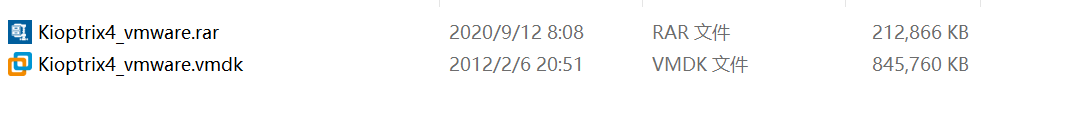
# 0x00:下载链接

下载地址: <https://www.vulnhub.com/entry/kioptrix-level-13-4,25/>

描述过长，总的来说就是获得root权限就行了



下载完以后解压发现只有一个.vmdk的文件，意味着这次要手动安装靶机了



# 0x01:安装靶机



然后点稍后安装操作系统



我这里的选择是Linux通用的Ubuntu版本也可以点其它



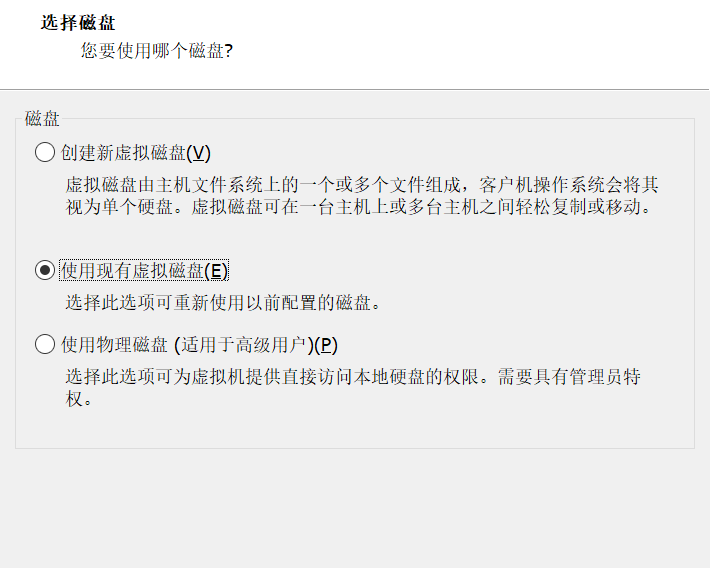
懒得改名



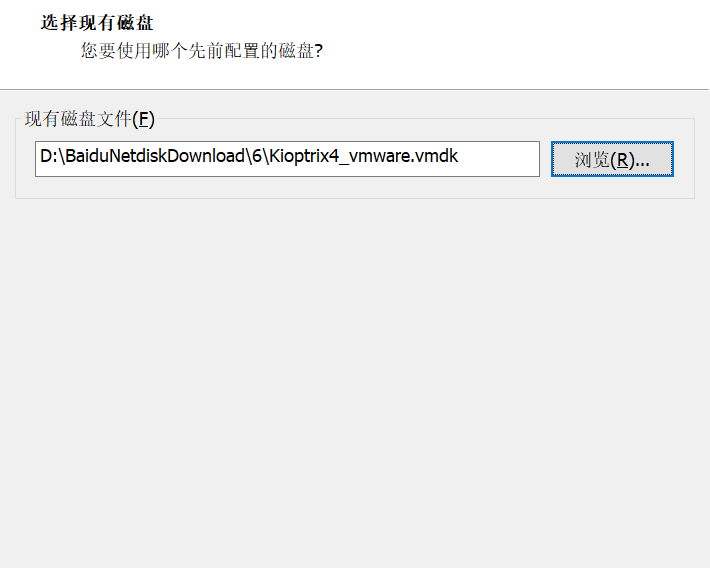
分配512MB就够了太多占用内存



这里是关键一定要选使用现有虚拟磁盘



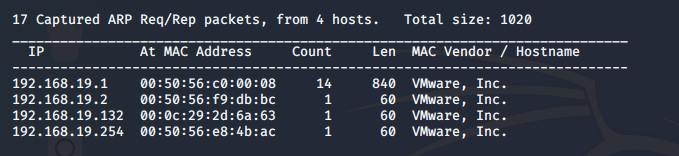
然后导入刚解压好的.vmdk文件就可以运行了



# 0x02:探测靶机

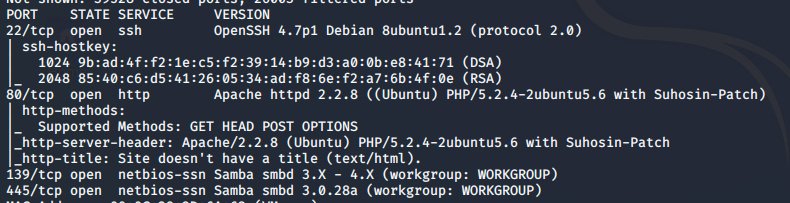
先用netdiscover探测一波，排除.1,.,2和.254默认IP可以确认靶机IP为192.168.19.132

命令:netdiscover -r 192.168.19.0/16

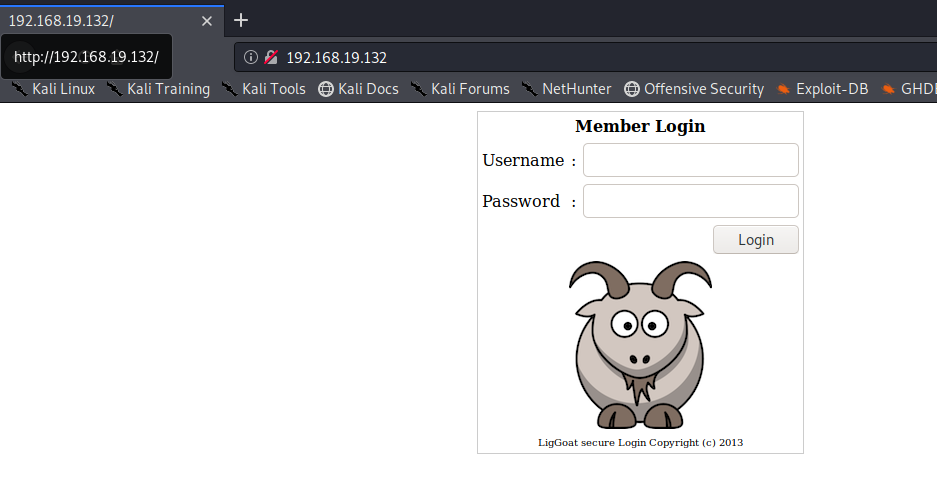


开始用NMAP探测波端口,主要开了22，80，139和445端口

命令:nmap -A -sS -sV -v -p- 192.168.19.132

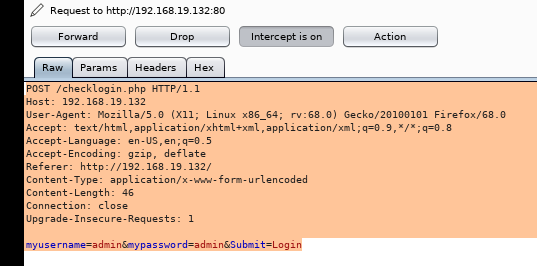


访问波IP可以正常回显，开搞



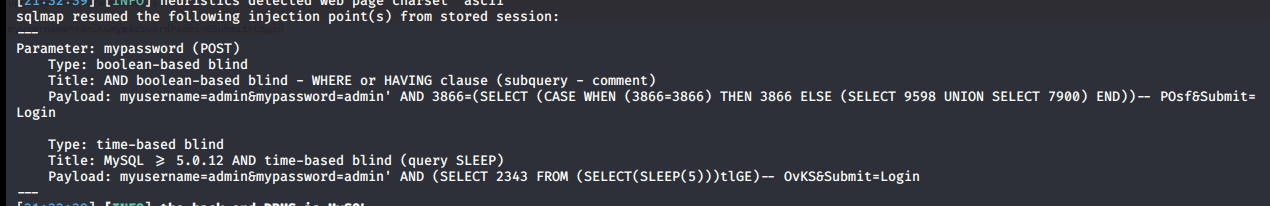
# 0x03:登录端口存在SQL

由于一上来就有个登录端口先用Burp抓个包然后送到sqlmap里面



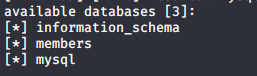
很容易就跑出来了

命令:sqlmap -r 5.txt –level 3 --batch



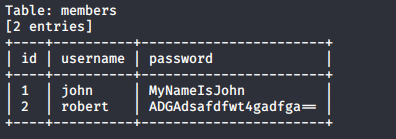
继续跟进得到3个库

命令: sqlmap -r 5.txt –level 3 --dbs --batch

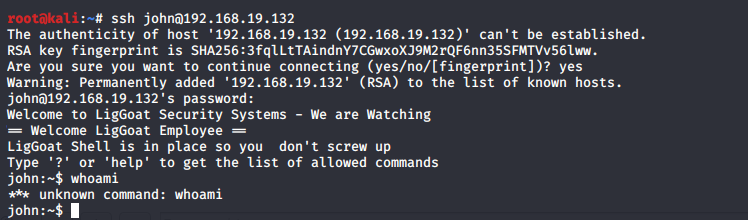


直接跑members里面的数据，得到两个账号但是robert的密码解不开。。。。

命令: sqlmap -r 5.txt –level 3 –dbs -D members --dump –batch

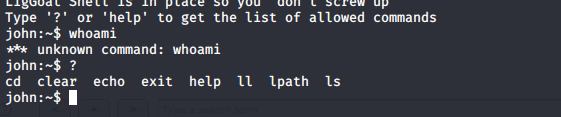


由于目前得到一个已知账号john外加开了22端口尝试输入，发现登录成功

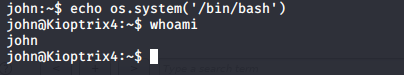


# 0x04:逃离限制shell

虽然现在登录进来了，但是发现能执行的命令非常少连whoami都执行不了，用?查看了一下只有8个命令可以执行，这种情况可能是遇到一个限制的shell

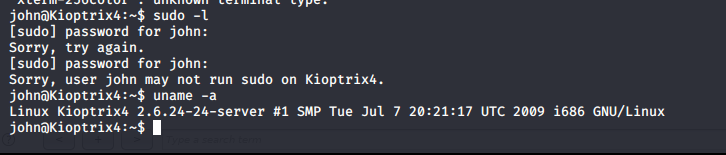


这里在网上查了一下<https://www.lshack.cn/653/>这篇文章有写各种方法逃离shell，因为目前位置我们能对应执行的只有echo，所以只能尝试echo os.system(‘/bin/bash’),成功跑路



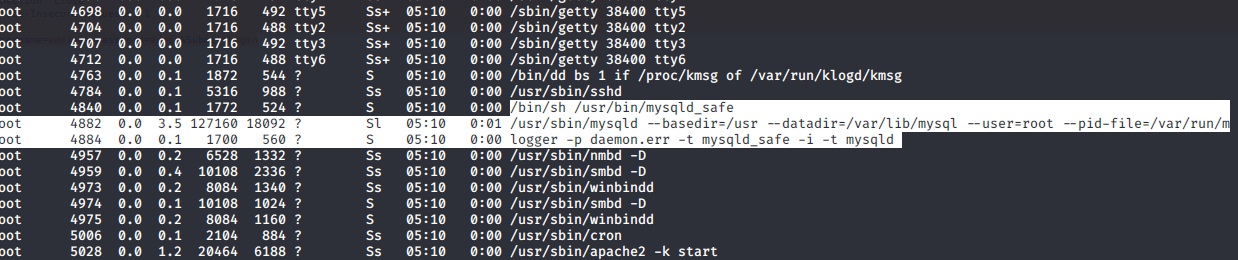
# 0x05:提权

先用sudo -l还是一如既往的失败，查看了内核版本结果发现gcc运行不了是最尴尬的。



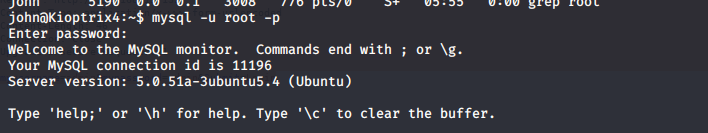
那么换种操作，查看具有管理员权限的进程,结果发现似乎mysql也有root权限

命令:ps aux | grep root

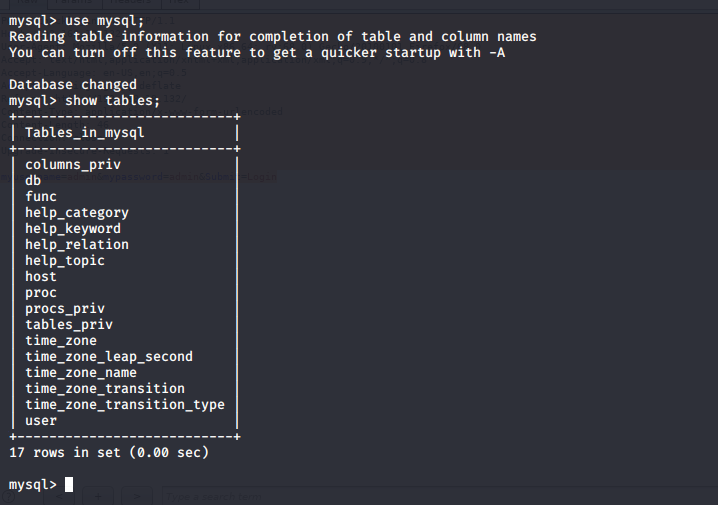


哦吼，MySQL有root权限那似乎是MySQL的UDF提权或者是MYSQL提权了我是参考了这篇文章[https://www.cnblogs.com/klown/p/11938064.html](https://www.cnblogs.com/klown/p/11938064.html还有这篇usermod) 顺便查了一下其它文章

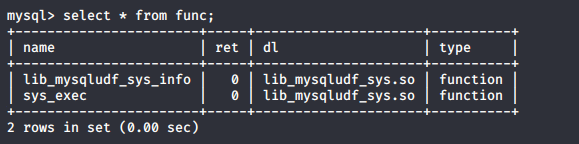
那首先先进入MySQL数据库先使用root root结果错了试了空密码才可以进来



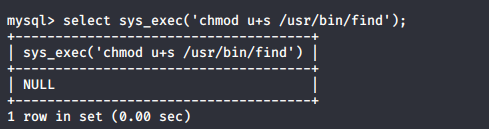
进入mysql数据库以后已经有个func的表继续



进入以后发现已经定义好了



开搞，赋予find一个root权限



然后去到/tmp目录创建一个文件名为makabaka,然后就是一个root权限了，然后在进入到shell模式去读取flag

