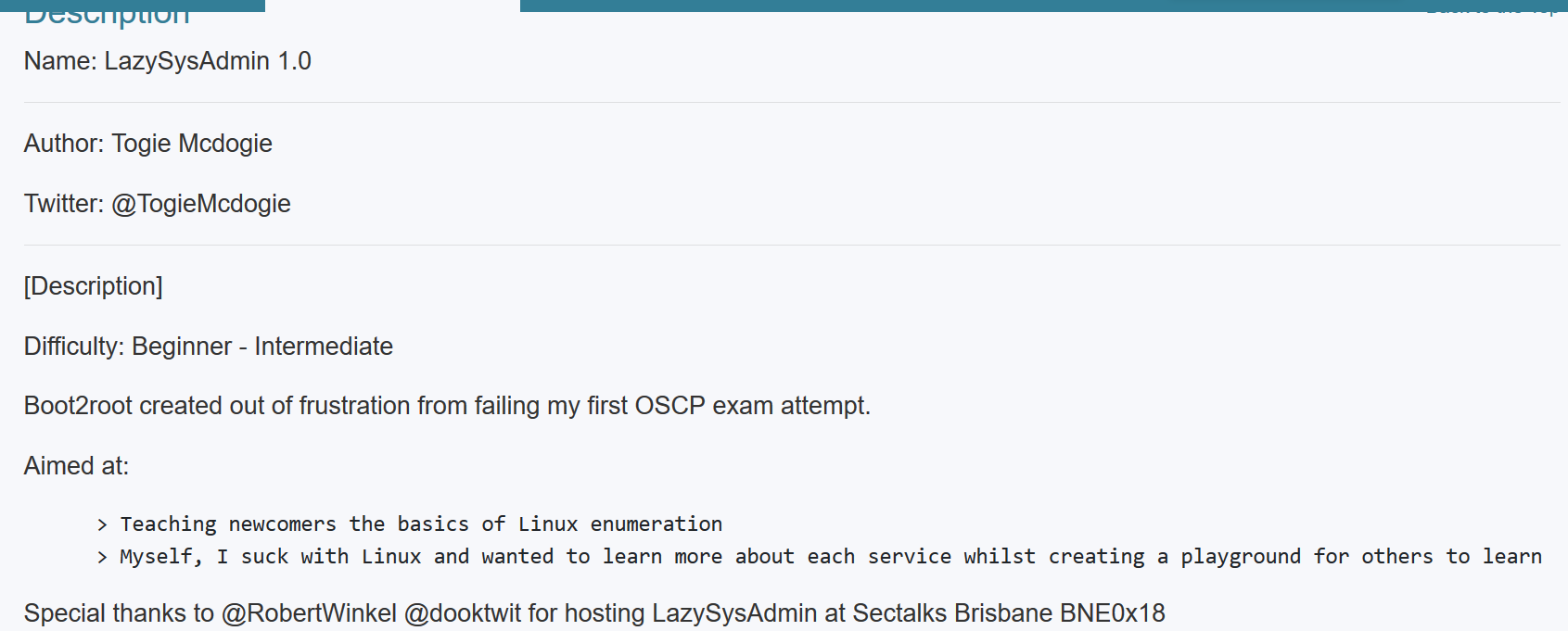
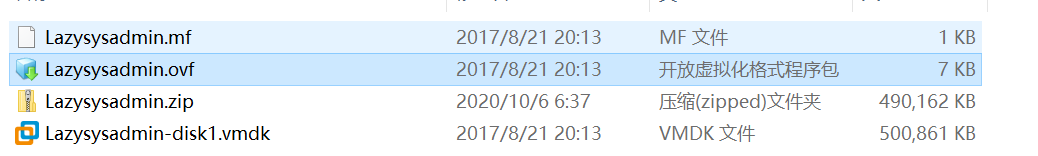
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/lazysysadmin-1,205/>

难度为新手到中等然后目的是了解基本的Linux枚举，还有了解一波各种服务



下载完后解压得到一个.ovf的文件



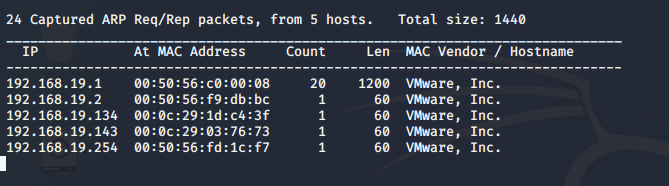
双击.ovf选择一个合适的位置安装，然后就可以运行了，已经默认调回NAT模式



# 0x01:探测靶机

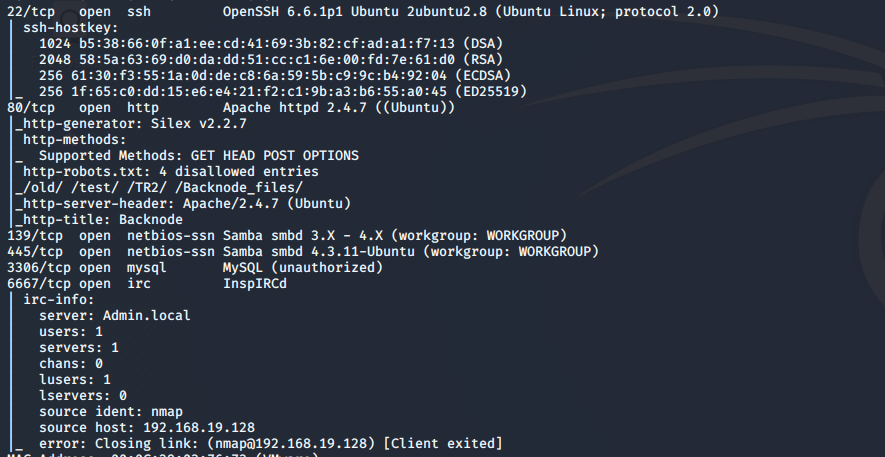
还是先使用netdiscover探测波靶机,排除.1,.2和.254可以确认靶机IP为192.168.19.143，192.168.19.134是我的kali 2020，我现在用的是2019

命令:netdiscover -r 192.168.19.0/16



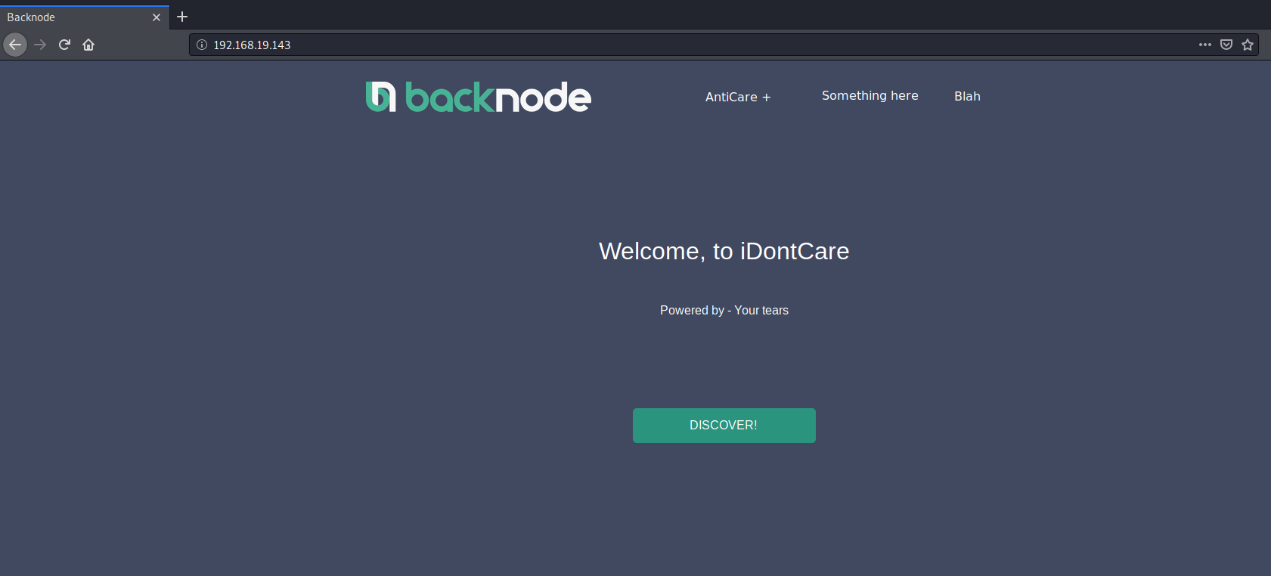
开始探测波端口,这次开放的端口比较多有22，80，139，445，3306和6667

命令:nmap -A -sS -sV -v -p- 192.168.19.143



这次的计划是这样子的兵分三路，我用kali 2020去尝试爆破波22端口时间为未知，然后检测波80端口是否正常如果正常的话，先去139端口用smbclient和enum4linux探测点smba信息回来，然后在集中精力在80端口

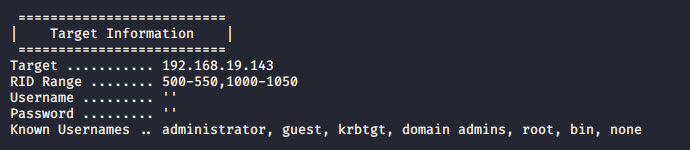
输入IP，页面回显正常

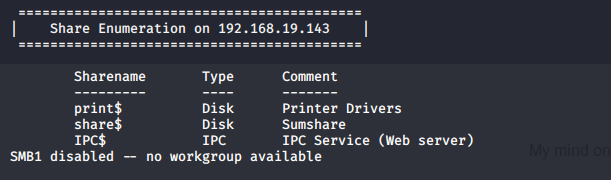


# 0x02:挖掘信息

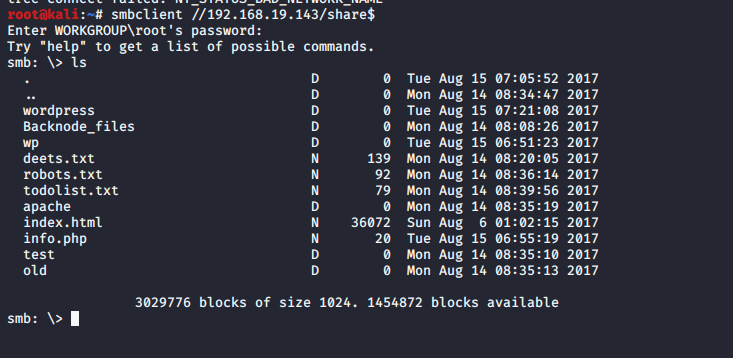
先用enum4linux扫点信息,可以看到有多个用户然后username 和password是’ ’,代表密码为空，然后第二可以得到一个目录有share$

命令:enum4linx 192.168.19.143

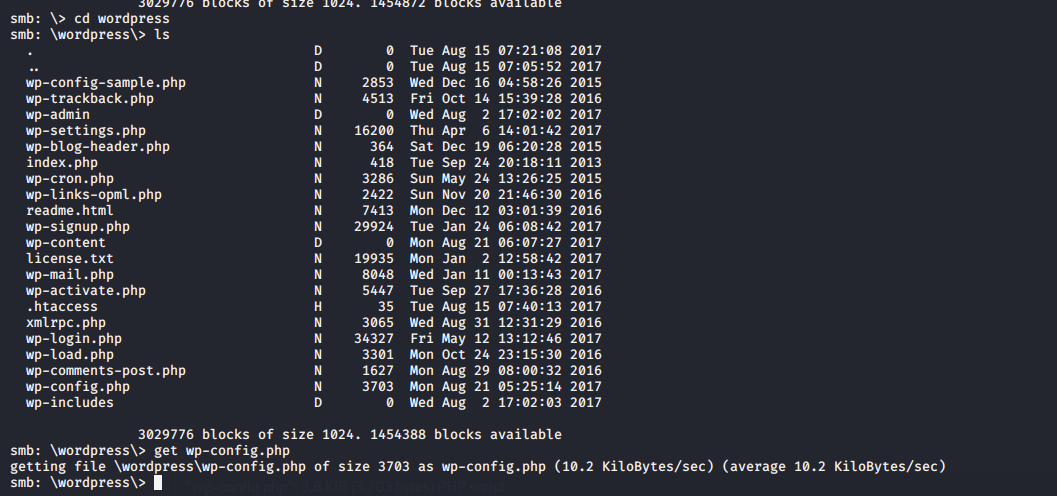




然后开始用smbclient连接一下，密码为空登录成功

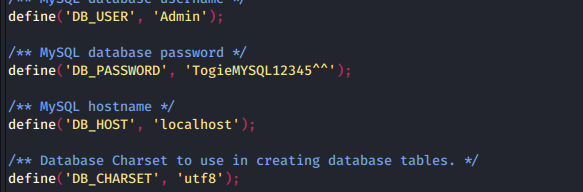


由于看到有个wordpress所以猜测可能是个CMS站点，进入wordpress发现有个wp-config.php用get下到本地

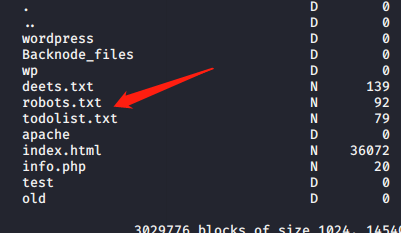


打开以后得到一个账号密码先不着急记录下来

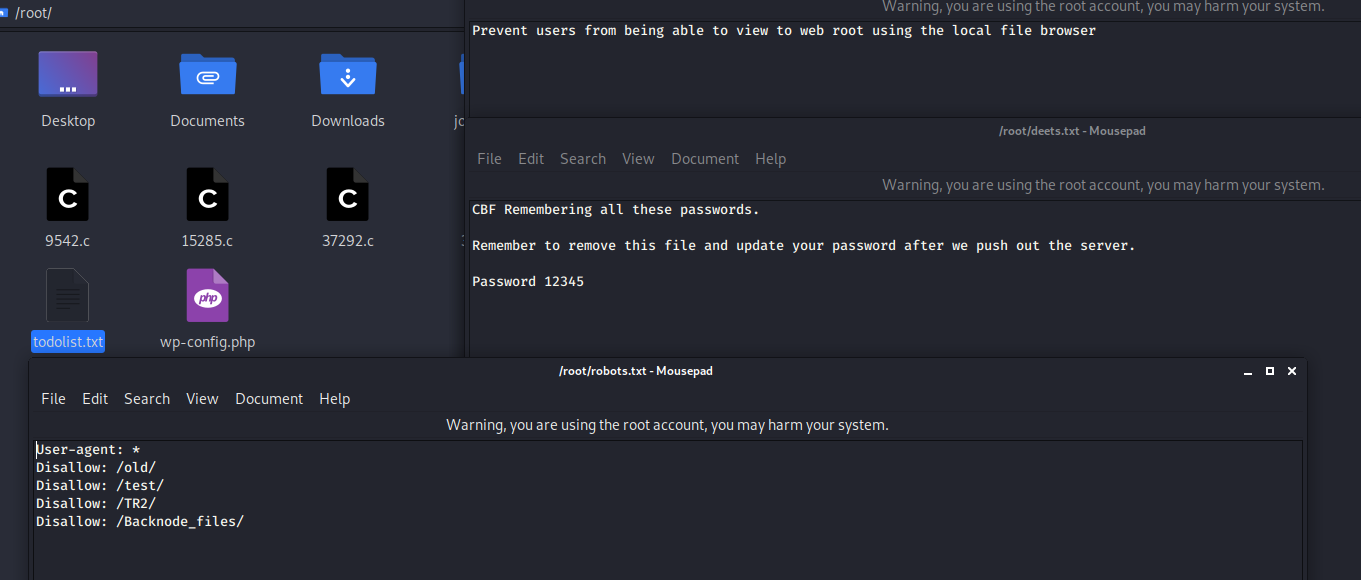
Admin TogieMYSQL12345^^



然后再回到主目录，这里有3个.txt的文件分别是deets.txt todolist.txt和robots.txt用get +文件名下载到本地

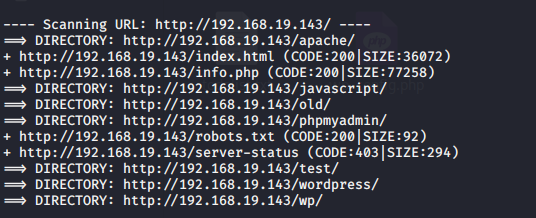


Robots.txt的信息就是4条路径，然后deets.txt有个关键词密码是12345，然后最后一个看到不是很明白防止用户使用本地浏览器直接看到web root ?

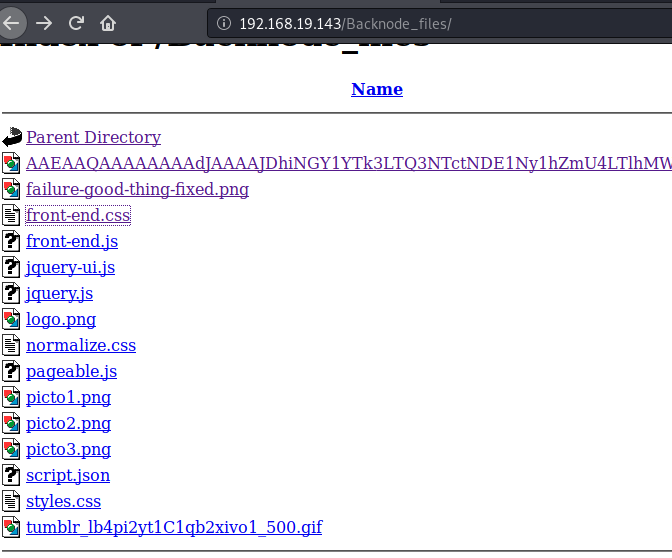


# 0x03:集火80端口

在Kali2020这里暂停一下，把密码指定为12345在跑一下，然后在2019的kali开始用dirb常规化跑跑挖到很多东西逐一跟进

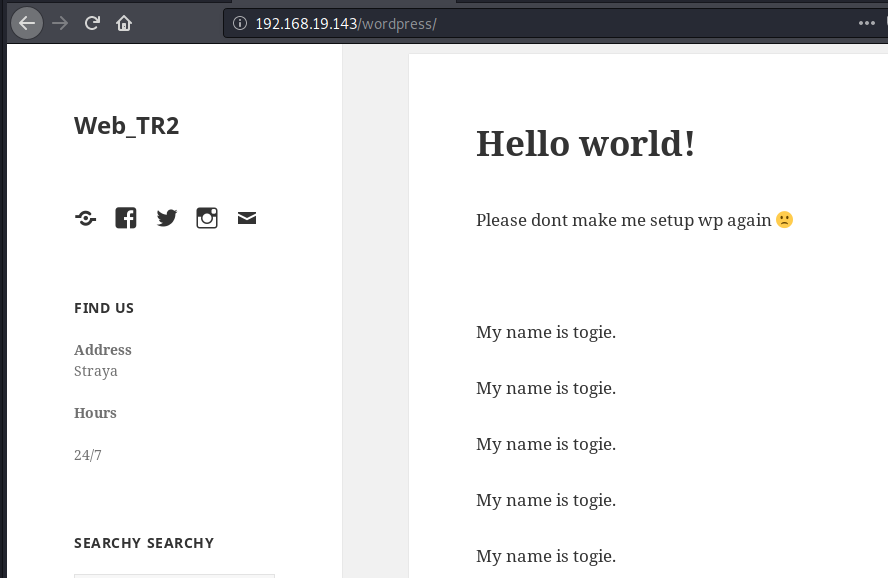


排除/old和/test里面为空，跟进/robots.txt跟刚才下载的东西一样也是有4条路径，在排除/TR2因为是403访问不了最后robots.txt里面只有一条路径可以用就是/Backnode\_files/然而里面都只是图片还有.css文件卒



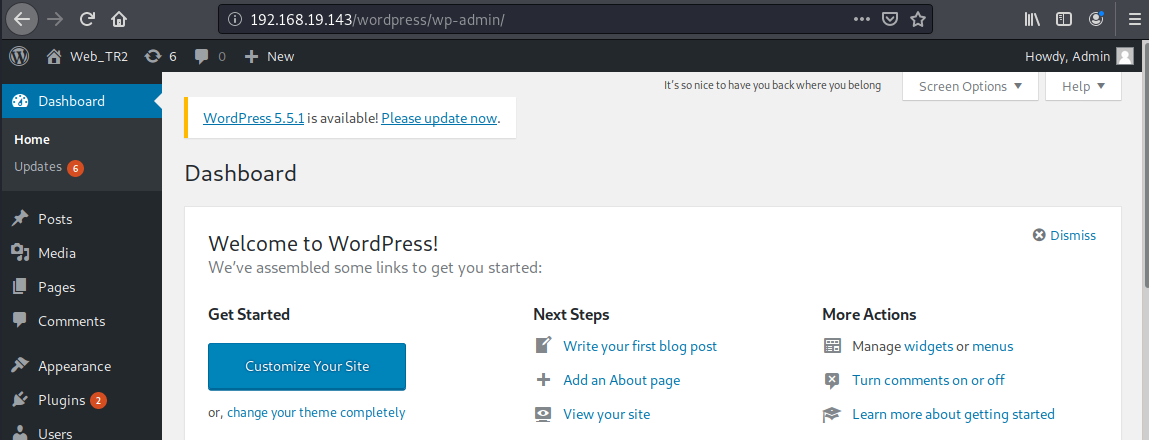
# 0x04:挖掘/WordPress信息

先跟进一波192.168.19.143看看会不会正常返回，免得又奔溃了，哦吼返回正常同时可以提取到一个信息togie可能是用户名，继续在kali 2020加多一个窗口用hydra 爆破togie用户



既然知道/wordpress页面正常运行尝试到后台登录处输入前面得到的账号密码

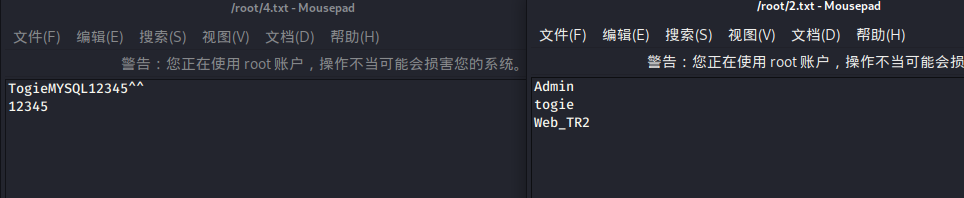
Admin TogieMYSQL12345^^成功登录



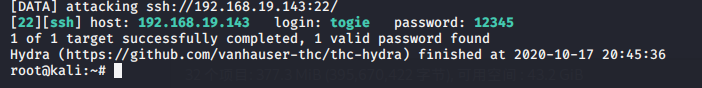
先整理一下手上目前知道的账号和密码,再跑一次SSH端口，这个不行等1小时我就考虑后台getshell了

已知账号:Admin togie Web\_TR2(可能是用户名)

已知密码: TogieMYSQL12345^^ 12345(不知道哪里的只是说server)



Emmmmm当场裂开原来12345是指SSH端口行吧



# 0x05:提权

用SSH登录以后提权很简单，直接sudo -l可以看到权限很高直接切换就可以了。爆破半天还不如用已知信息爆破

