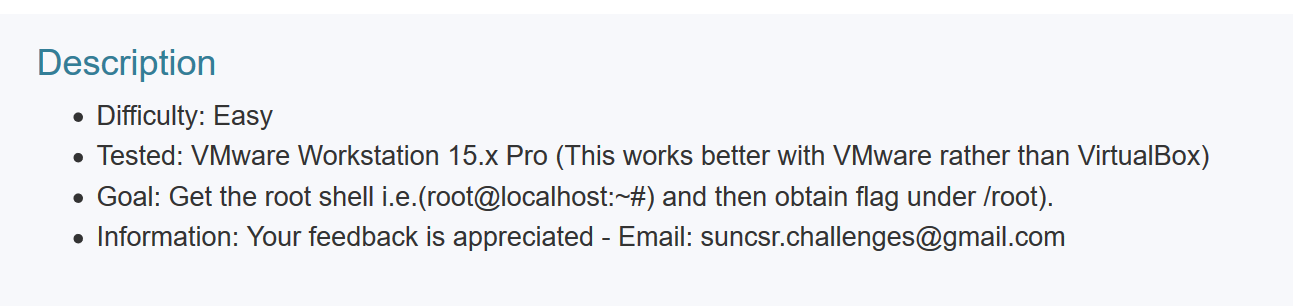
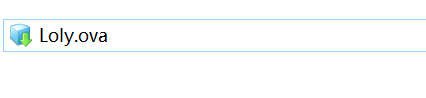
# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/loly-1,538/>

难度为简单，建议用VMware来做，目标是获得root的shell



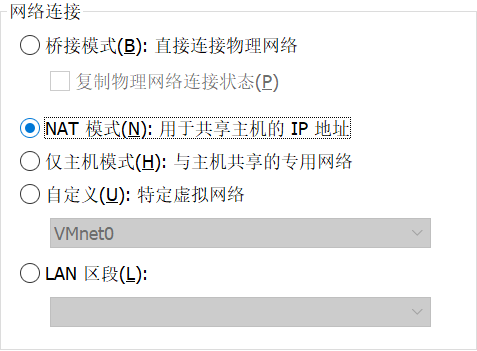
下载完以后是个.ova文件



选择一个合适的地方存放



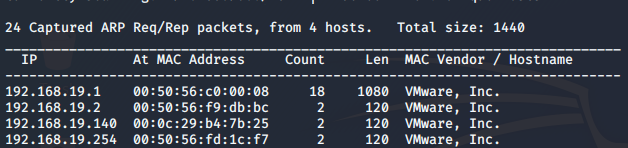
记得调回NAT模式，点击运行就可以开始攻击了



# 0x01:探测靶机

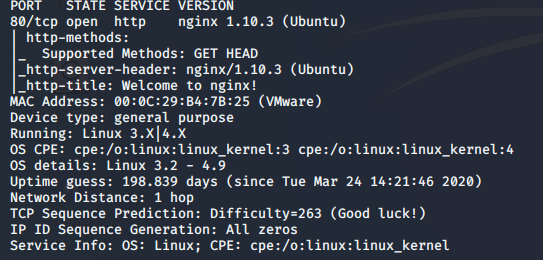
还是先用netdiscover探测波靶机IP,排除.1,.2和.254可以确认靶机IP为192.168.19.140

命令:netdiscover -r 192.168.19.0/16

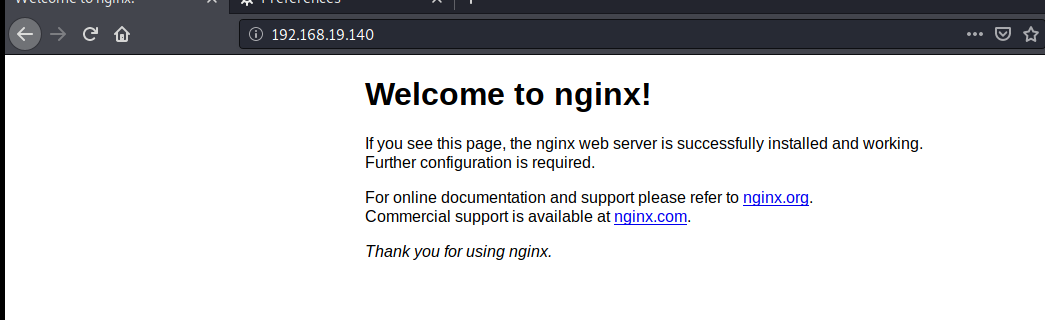


然后开始用nmap探测波端口,这次开放的端口比较少，只有80

命令:nmap -A -sS -sV -v -p- 192.168.19.140



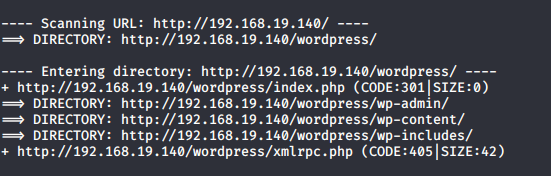
访问波IP可以正常访问开搞



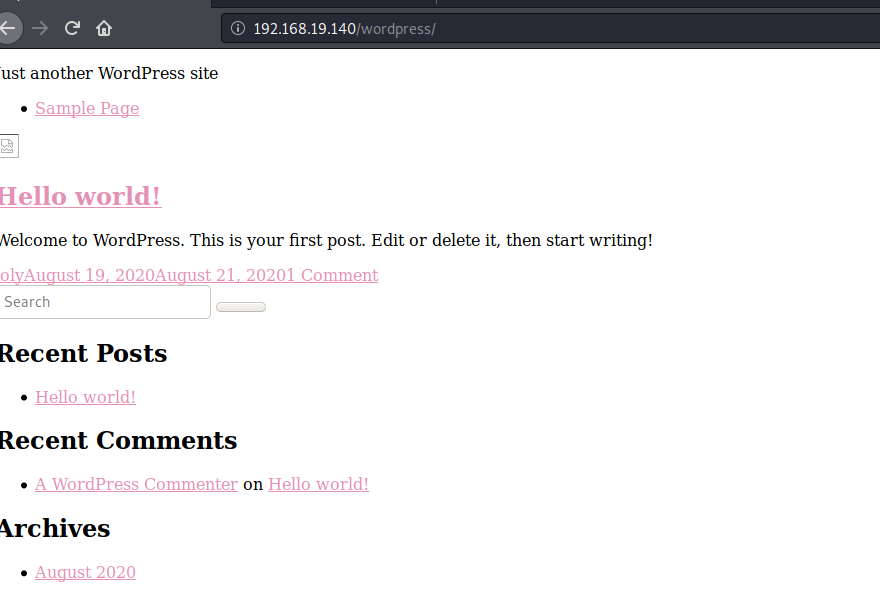
# 0x02:挖掘信息

先用dirb探探路,发现一个/wordpress，可以确认目标靶机是WordPress站点

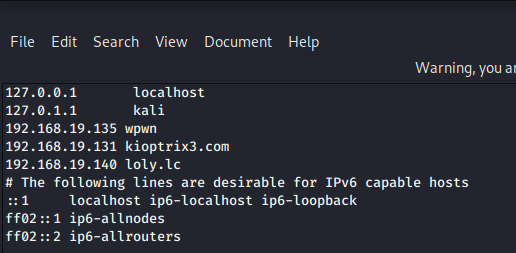
命令:dirb http://192.168.19.140



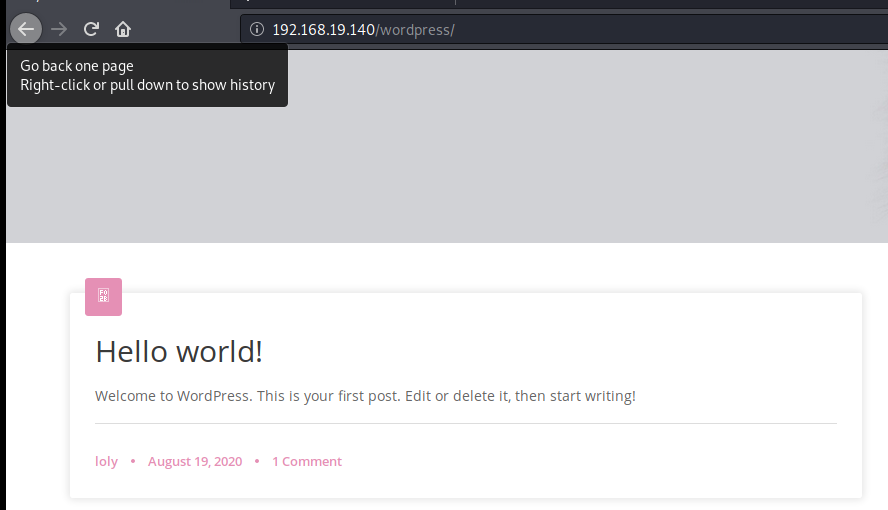
跟进一波站点发现乱码得修改一波/etc/hosts



这里添加一波IP地址和名字



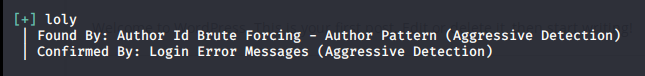
再次查看时，页面正常回显



# 0x03:利用wpscan获取信息

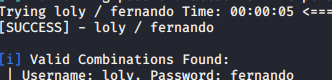
开始用wpscan扫一波用户名,扫到一个Loly的用户名

命令:wpscan –url <http://192.168.19.140/wordpress> -eu

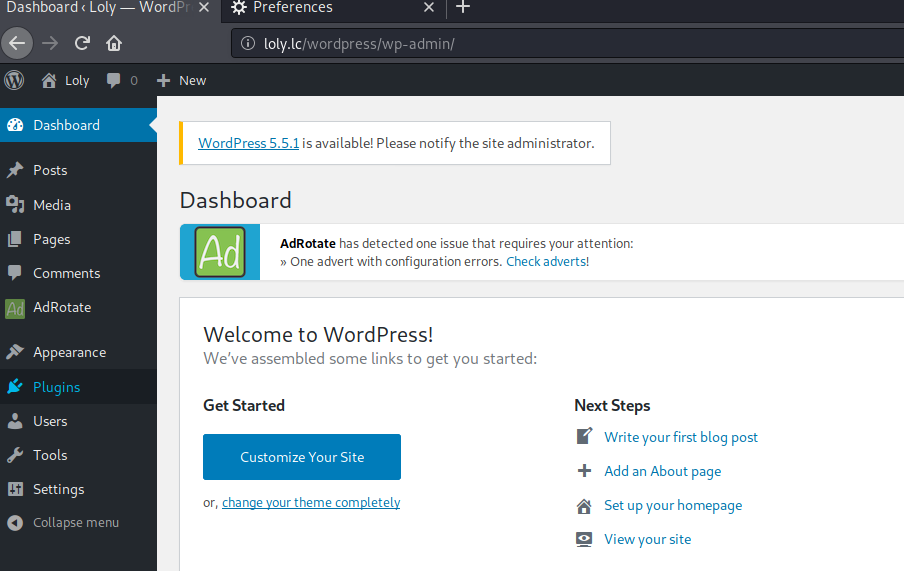


然后尝试一波爆破密码,最后爆出来是 /fernando

命令: wpscan --url http://192.168.19.140/wordpress -P /usr/share/wordlists/rockyou.txt -U loly

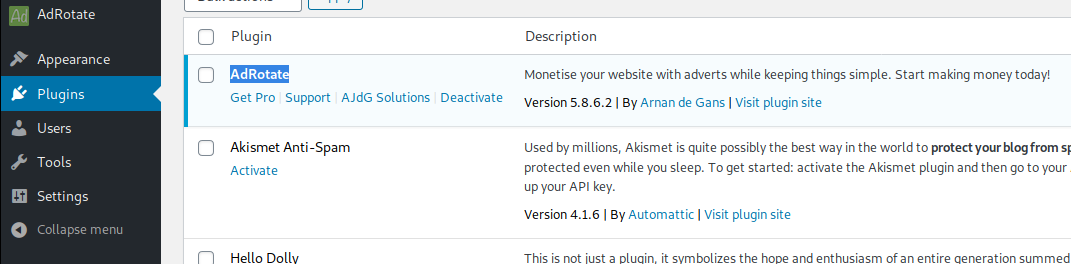


成功登录

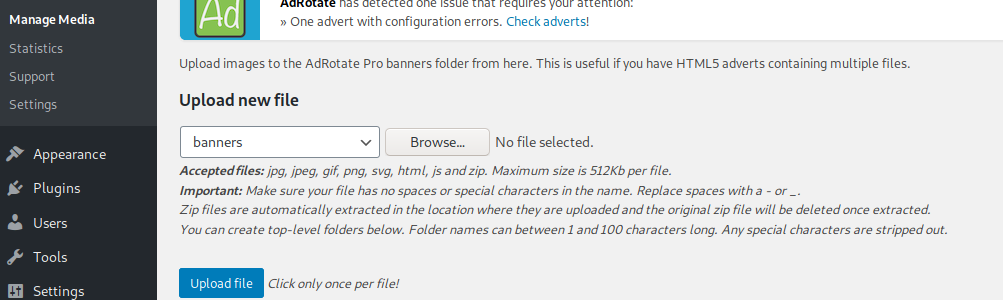


# 0x04:尝试getshell

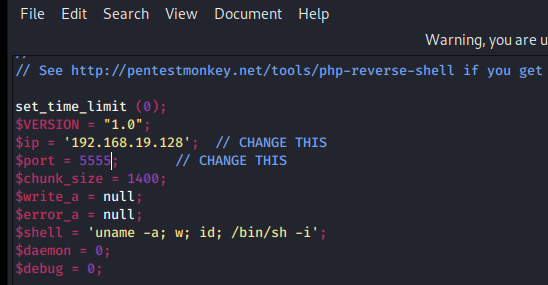
这里在插件这里发现一个AdRotate的东西



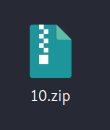
AdRotate有很多功能，在慢慢点到Manage Media的时候找到一个上传新文件的功能点。突破点来了，可以接受zip之类的格式，开始准备反弹shell



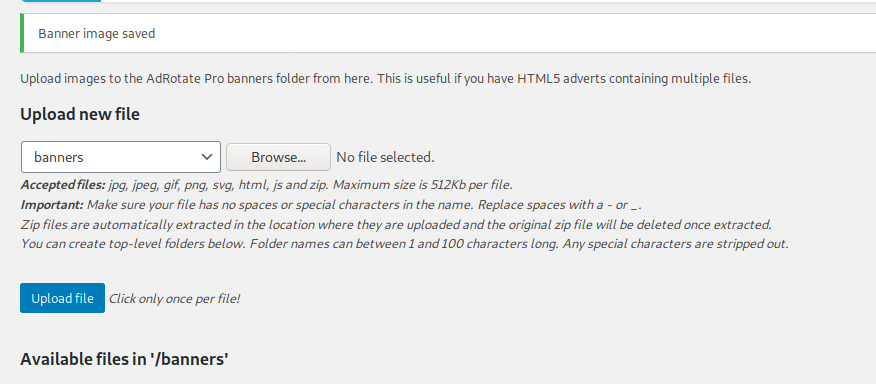
把kali的自带反弹shell的文件改波IP和端口



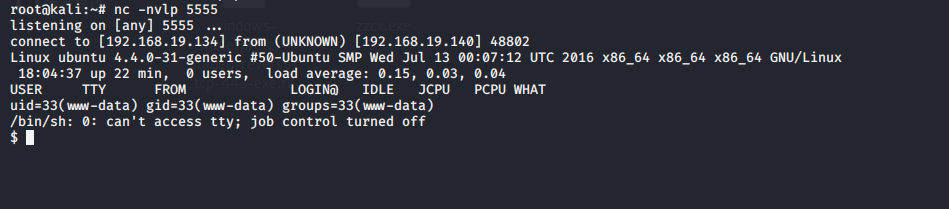
经过实验，还是先要把反弹shell打包进zip



上传完以后这里会提示available files in /banners,所以得去banners找一波

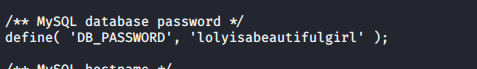


最后访问192.168.19.140/wordpress/wp-content/banners/10.php,记得提前开启netcat反弹成功

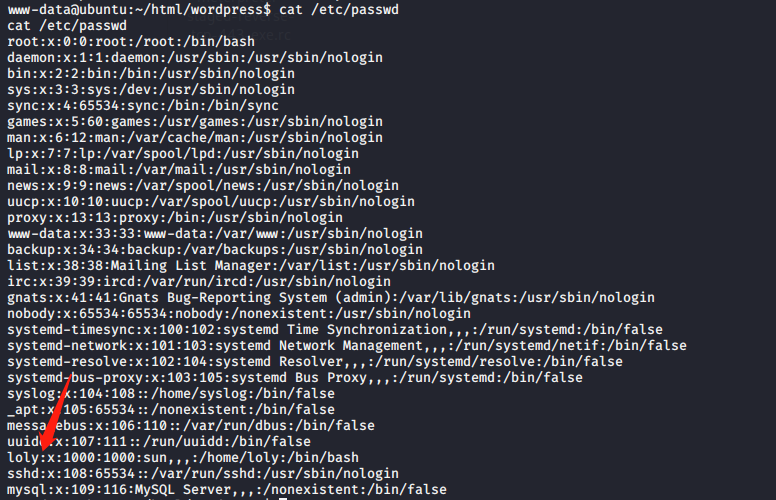


# 0x05:挖掘信息

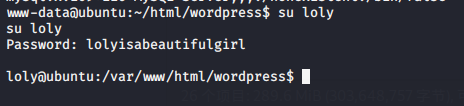
挖掘一波信息，由于现在的用户是www-data,我们的目标是挖掘信息变成一个正常的用户，在提权变成root来到/var/www/html/wordpress目录下，cat一波wp-config.php得到一个密码



然后cat /etc/passwd查看一波用户名，找到一个loly

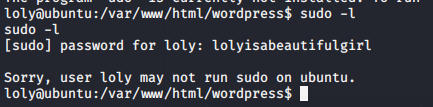


切换用户一波，偷渡成功

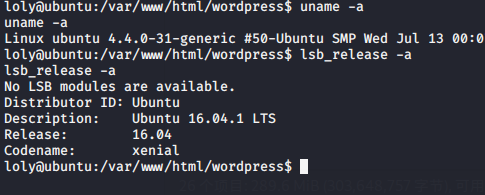


# 0x06:提权

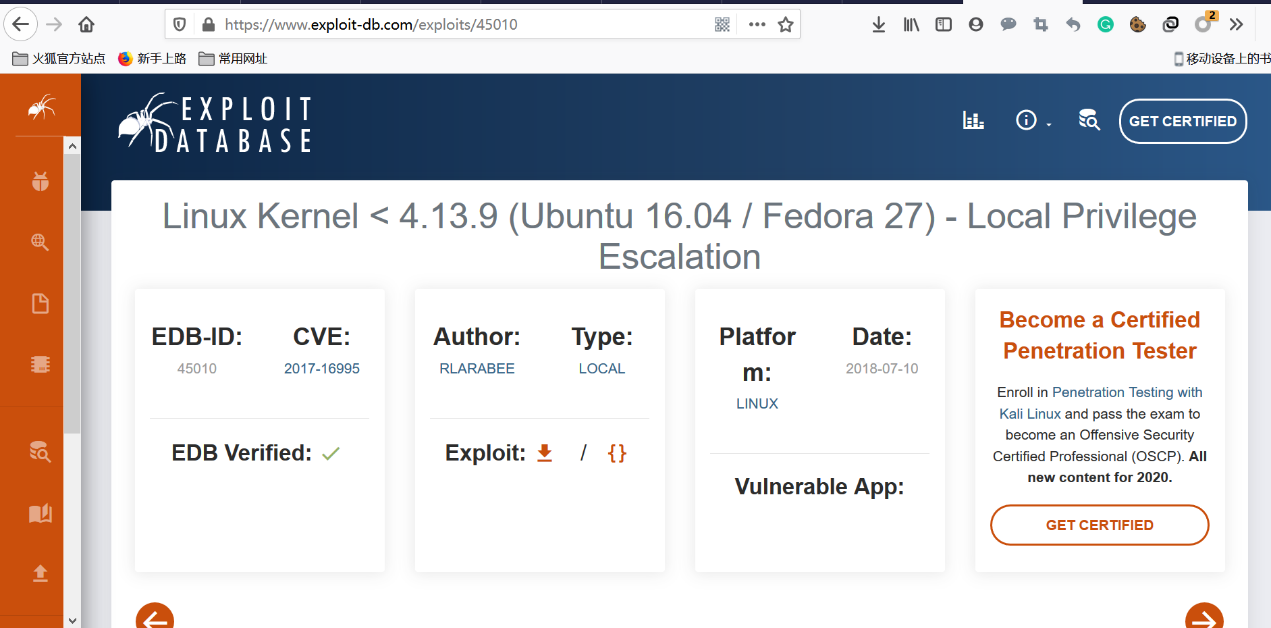
Sudo -l还是倒了



换成uname -a 和 lsb\_release -a提取关键词收集信息



在exploitdb找到这个



下载下来，顺便开启Python共享模式



上传，gcc编译，提权成功

