# 0x00:靶机下载

下载链接: <https://www.vulnhub.com/entry/ai-web-1,353/>

难度为中等，目标就是拿到root的flag



下载以后解压有个文件夹跟进



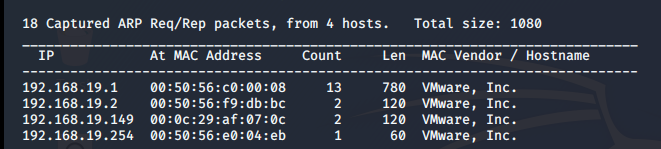
然后点开.vmx就会自动打开VM调成NAT模式了，直接运行就可以了



# 0x01:探测靶机

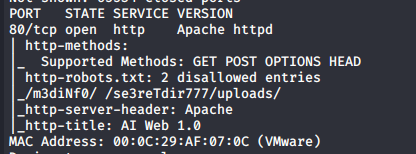
先用netdiscover确定一波靶机IP,排除.1,.2可以确定靶机IP为192.168.19.149

命令:netdiscover -r 192.168.19.0/16

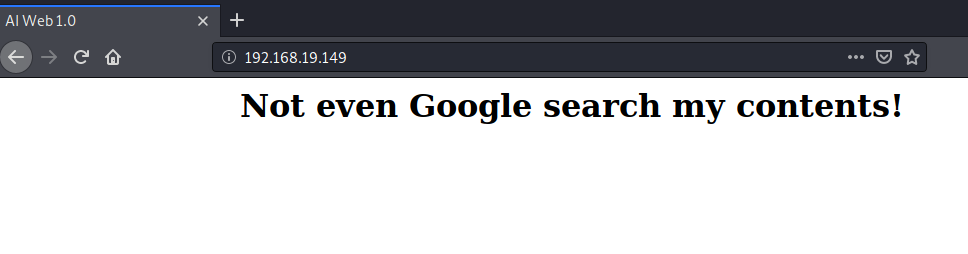


然后用Nmap探测一波端口，这次只开了80端口有点少

命令:nmap -A -sS -sV -v -p- 192.168.19.149

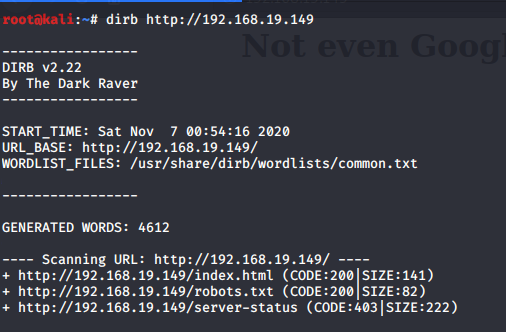


访问IP一波可以正常回显开挖

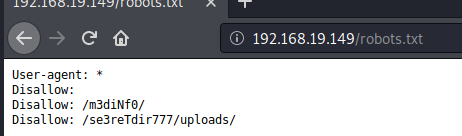


# 0x02:挖掘目录

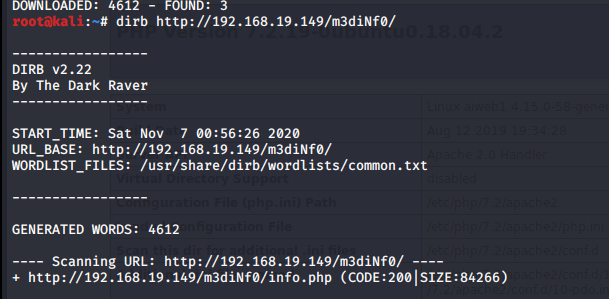
这里首先使用dirb挖掘一波，结果只发现个robots.txt比较有用



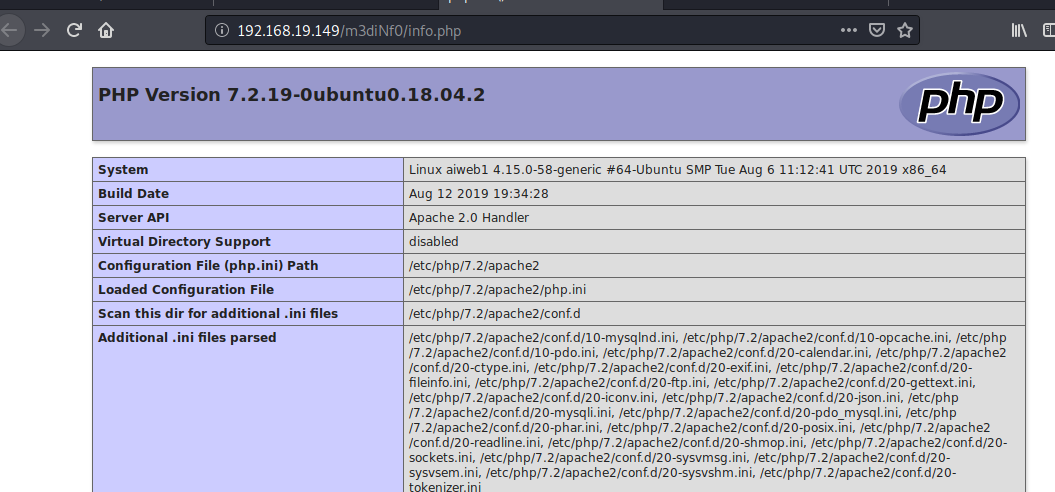
跟进发现有隐藏目录指向



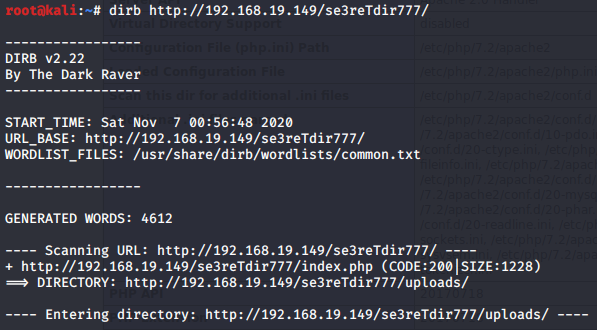
为了挖掘更多的东西继续挖掘更多的东西，继续用dirb扫/m3diNf0目录，扫到了一个info.php



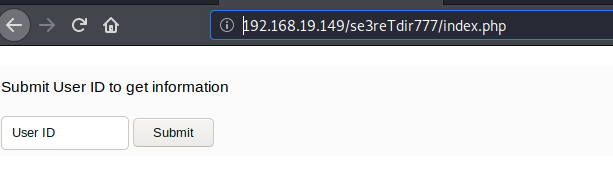
可以知道PHP版本以及往下翻的话可以找到绝对路径



扫se3reTdir777/可以找到一个index.php但是不知道为啥uploads访问不了

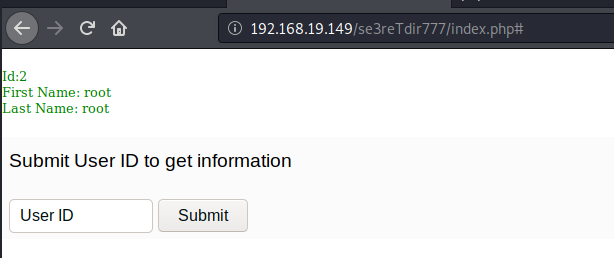


Index.php好像是一个查询的东西

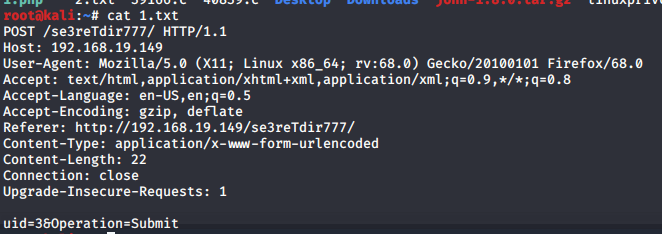


# 0x03:挖掘SQL漏洞

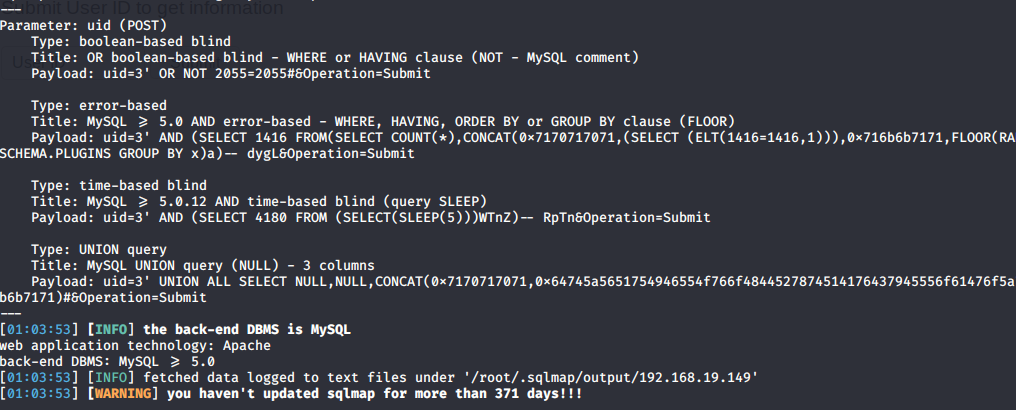
这里在user id输入了1和2发现可以显示点东西出来



尝试用burp抓包保存下来一波，可以尝试一下POST注入一波

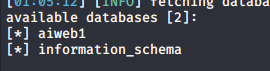


然后放到sqlmap里面成功跑出来

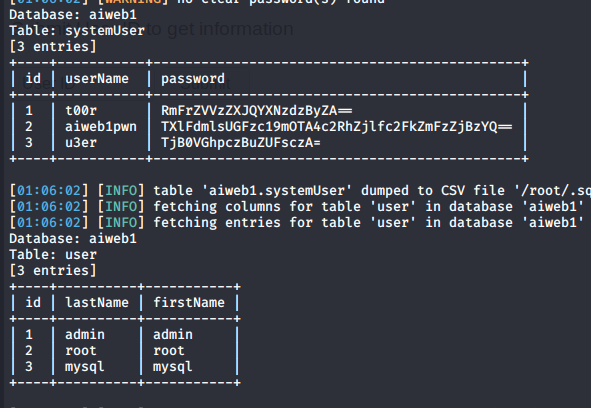


跟进一下,发现两个数据库，果断选择aiweb1

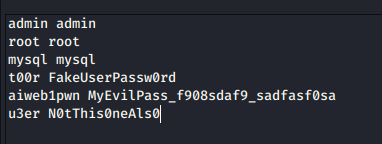
命令: sqlmap -r 1.txt –dbs



这里狠一点，由于是自己的靶机直接—dump得到两个表，而且都是用户密码



这里通过解码得到以下账号密码



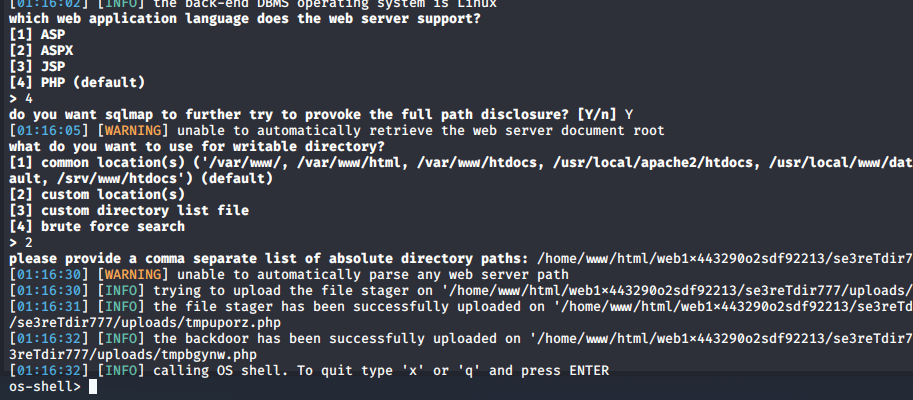
# 0x04:利用sqlmap获得shell

Sqlmap其实也是可以写shell的满足条件为dba为true或者知道绝对路径，这里回到info.php页面一直往下拉在DOCUMENT\_ROOT这里可以看到绝对路径



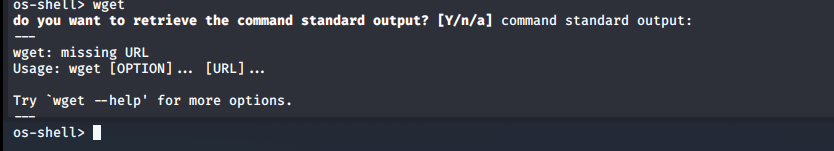
然后在sqlmap里面开始用—os-shell功能，选择php,然后选择2，输入绝对路径成功getshell

绝对路径: /home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads/(这里尝试了以下只有se3reTdir777/uploads才有写入权限)

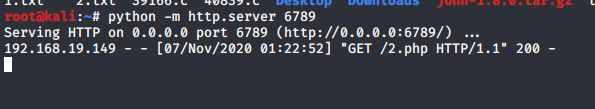


# 0x05:更换shell

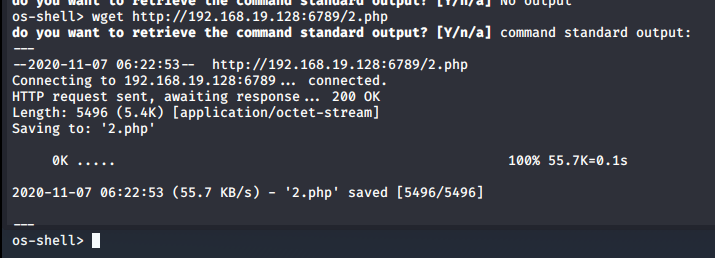
虽然现在有shell了，但是sqlmap有点笨，每次都会问你do you want to retrieve the command ?所以得更换一波变成反弹shell，想要获取反弹shell可以利用echo 写入一句话用菜刀连接再传一句话，这里我偷懒，我发现wget可以利用，那么可以直接在kali上传反弹shell在访问就行了



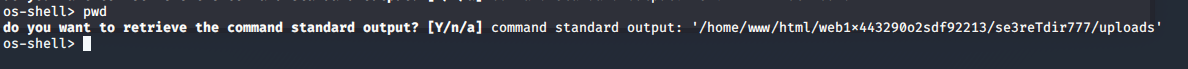
这里先准备好反弹shell,改成自己的IP以后开启共享模式



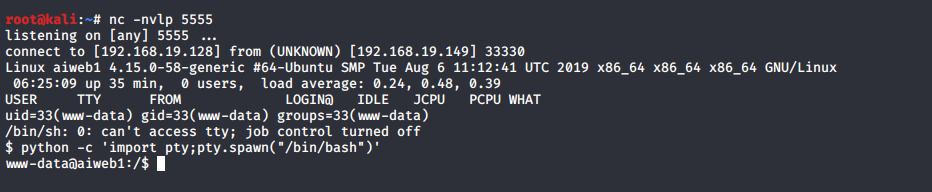
然后在sqlmap那里用wget下载好，如果没有反应就再来一次



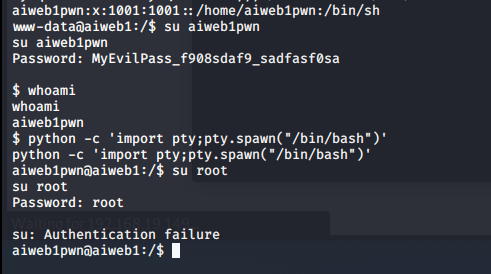
因为我们的当前路径是在/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads，同时我们把反弹shell下载到当前路径了，虽然uploads访问不了，但是不代表它目录下的东西也是不可以



记得提前开启nc,在前端访问/home/www/html/web1x443290o2sdf92213/se3reTdir777/uploads，更换shell成功

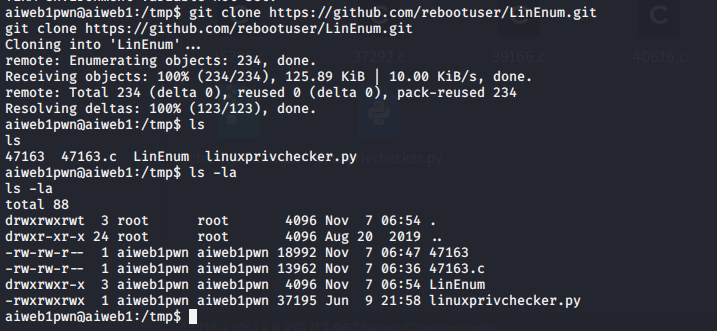


这里我在用cat /etc/passwd的时候，看到一个aiweb1pwn的东西哦吼，跟刚才SQL挖到的用户名重叠，直接su+输入密码成功，然而当我想切换成root的时候。。。。。。。结果是想屁吃

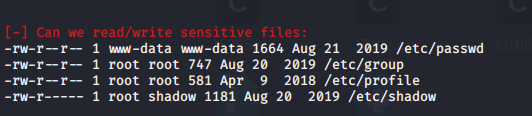


# 0x06:提权

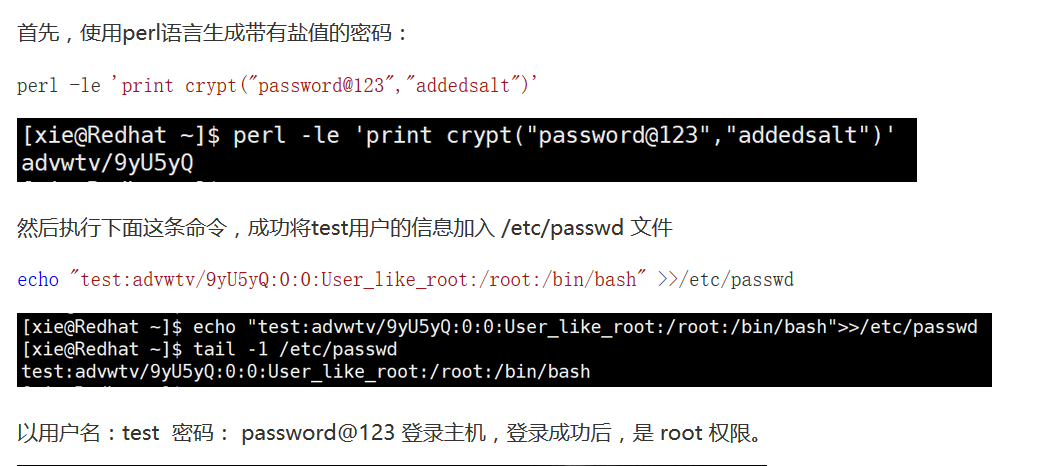
由于sudo -l 失败,find 失败，uname 失败，这里我直接在靶机上用git下载了一个提权辅助器 LinEnum



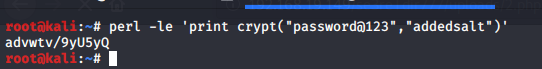
然后进入目录给波权限777运行emmmm好像没必要切换用户。。。。 可以看到可以以www-data写入/etc/passwd里面裂开



这里我用了网上的方法<https://www.cnblogs.com/csnd/p/11807647.html>



现在kali本地用perl生成一波密码



然后在靶机上用echo写进etc/passwd里面



最后直接su切换成root权限成功

