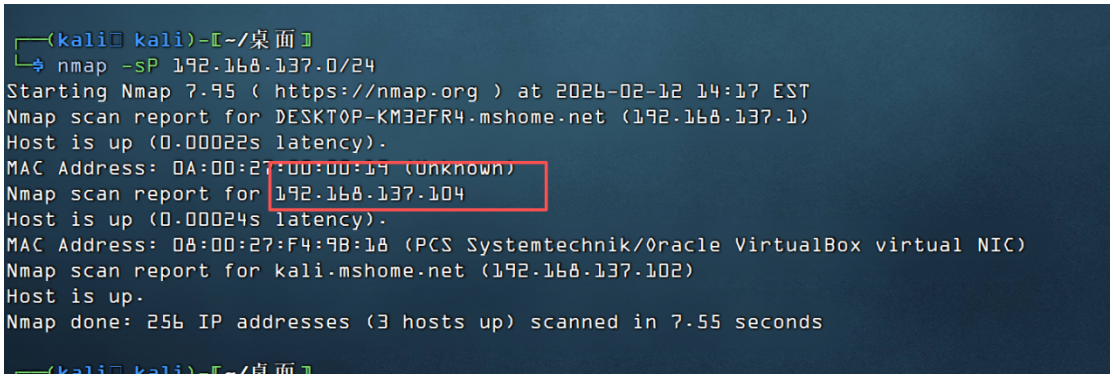
The_magician-12138

1.探测 IP

nmap -sP 192.168.137.0/24

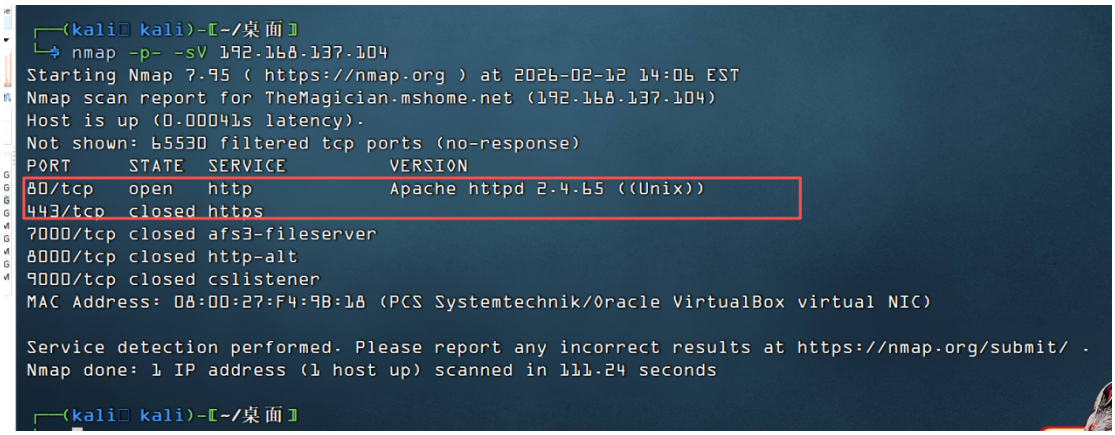


靶机 IP 是 192.168.137.104

2.扫描 IP

1)扫描端口

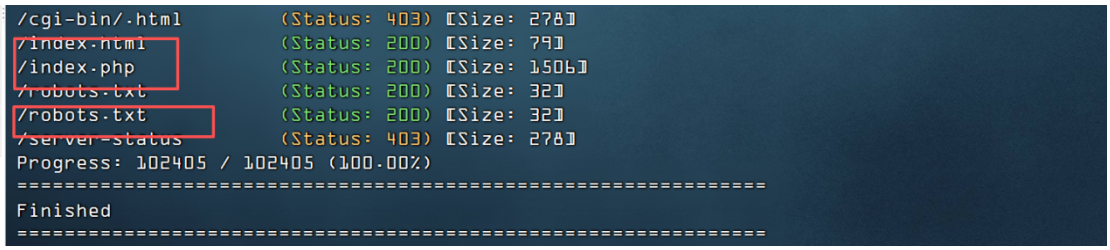
nmap -p- -sV 192.168.137.104



端口只有一个 80 端口

2)扫描目录

gobuster dir -u http://192.168.137.104 -w /usr/share/seclists/Discovery/Web-Content/big.txt -x php,txt,html,zip



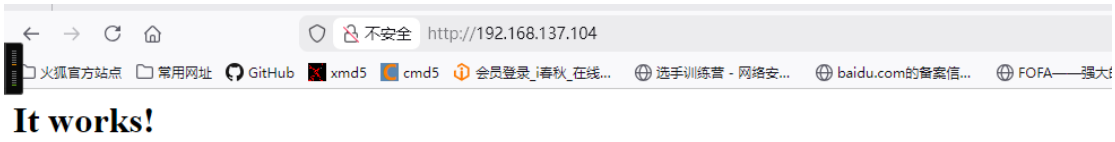
Index.php——靶机查询系统

Robots.txt——scanch.php

3.访问 IP

我们访问 80 端口

http://192.168.137.104/



查看源代码，没有什么信息

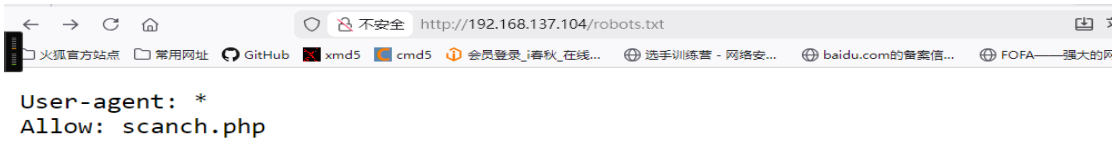
4. 渗透测试

1) 访问目录

http://192.168.137.104/index.php

是一个靶机查询系统

http://192.168.137.104/robots.txt



我们去访问 scanch.php

http://192.168.137.104/scanch.php

我们可以看到 2 个查询系统，我们去抓包测试是否存在 SQL 注入，发现 2 个页面都没有的。

2)SQL 注入

既然我们没有发现 SQL 注入，那么我们不要去输入任何东西，然后点击执行搜索和查询，我们去看源代码

突然在 index.php 源代码里面发现了<!--scanch_bate.php -->，我们必须去点击查询，然后查看源代码就可以看到 scanch_bate.php

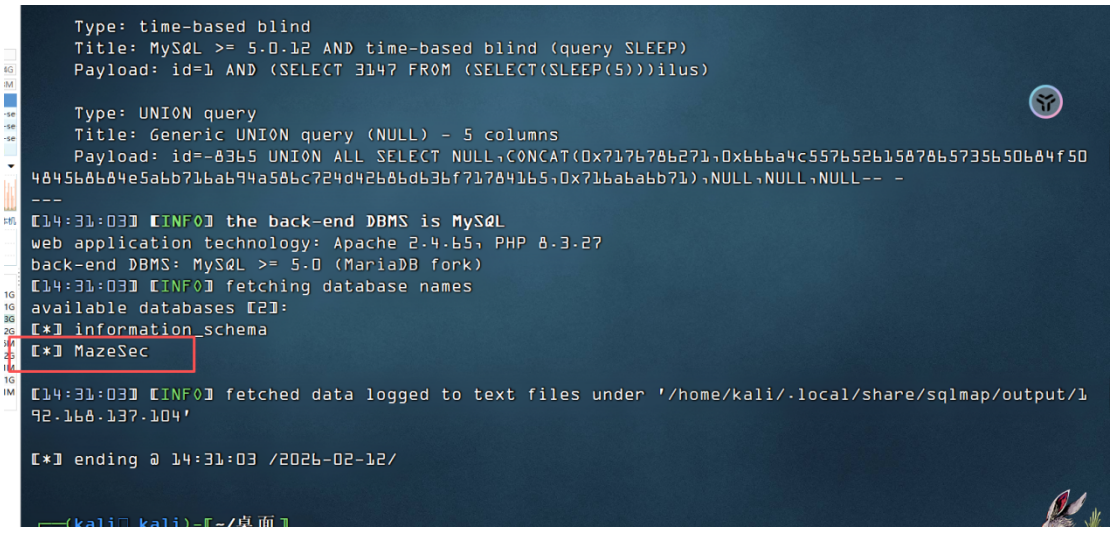
那么我们去访问这个页面

http://192.168.137.104/scanch_bate.php

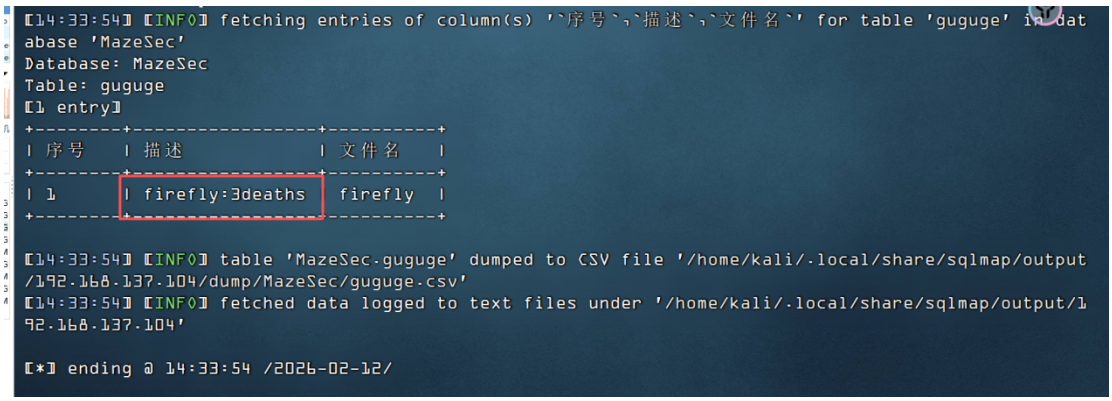
可以看到又是一个输入框，告诉我们去输入 1,我们猜测存在 SQL 注入,我们去抓包测试注入

发现存在 SQL 注入的

sqlmap -r 1.txt --dbs --batch



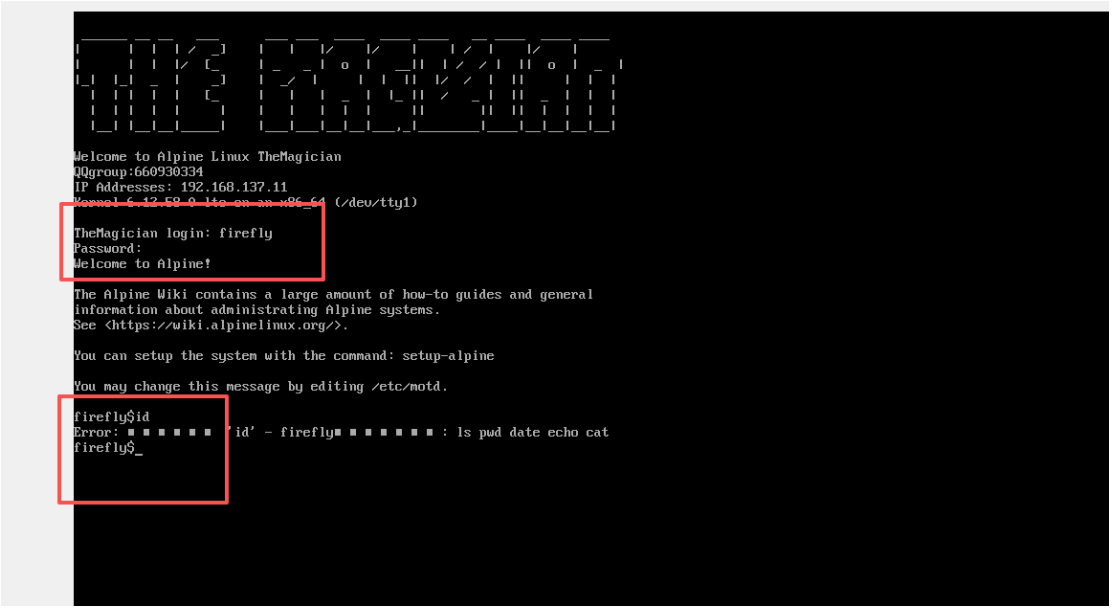
可以看到一个数据库，我们去爆破，最后爆破出来一组用户名和密码



3)登录系统

我们获取了用户名和密码，但是我们没有登录页面，那么我们只能把目光移到靶机界面了(因为目前只有这里能够登录了)

我们试试能不能登录成功吧

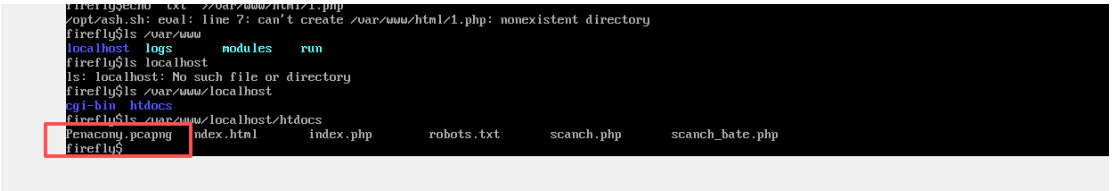


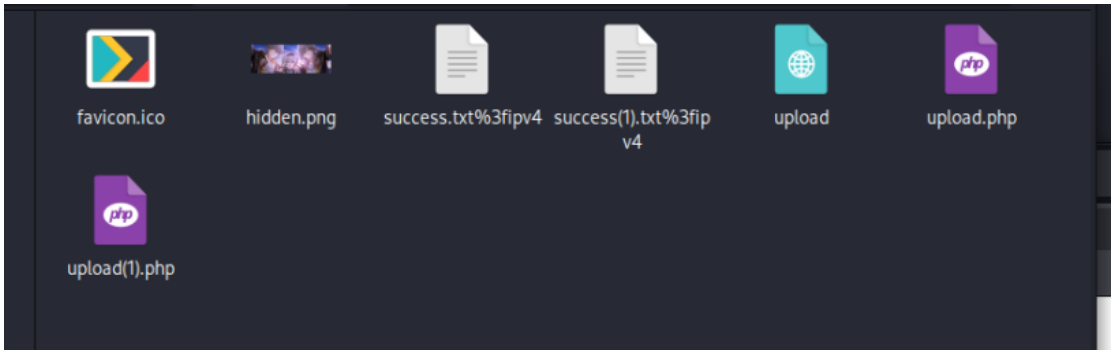
我们可以看到登录成功的，但是命令是受限制的，

我们使用的命令只有 ls pwd date echo cat

我本来的思路是在/var/www/html/里面写入一句话木马，然后去连接蚁剑，但是发现没有/html 目录，发现了 localhost 目录

在 localhost 目录下发现一个流量包，下载下来查看，发现没有什么用(我们去导出 http.request and http.request.method == "POST" 发现里面有一个图片，upload.php 等等，但是对于我们解题没有任何的帮助)



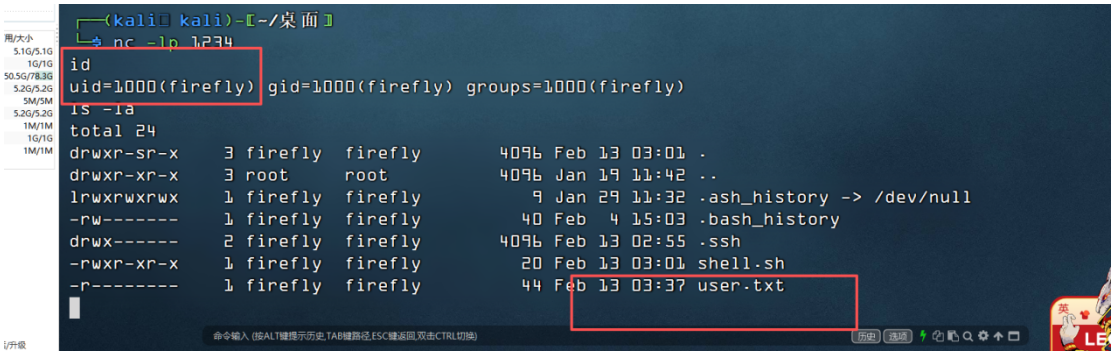


我们去写入结果发现没有权限，那么我们只能想办法看看能不能反弹 shell 了

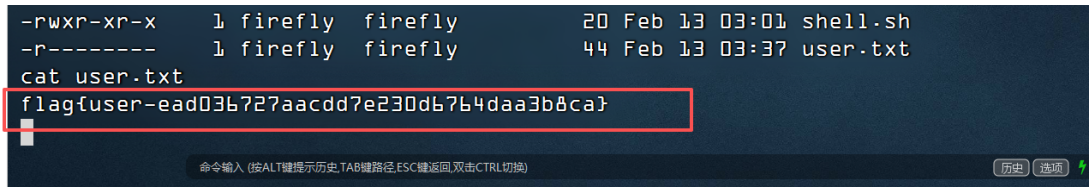
4)反弹 shell

我们直接去反弹 shell，是不会成功的

我们在前面加入 ls,即可反弹成功的，这里的 shell.sh 是我前面做题留下来的，里面只有一个 user.txt，我们可以看到没有报错，我们去看看有没有反弹成功吧



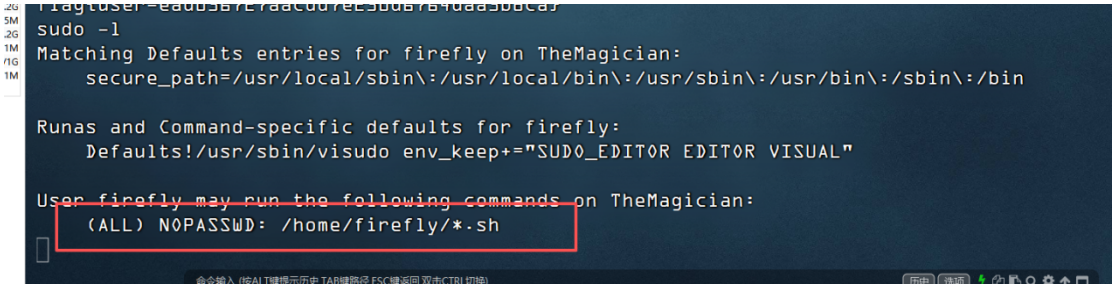
我们可以看到反弹成功的，我们去读取 user.txt 即可



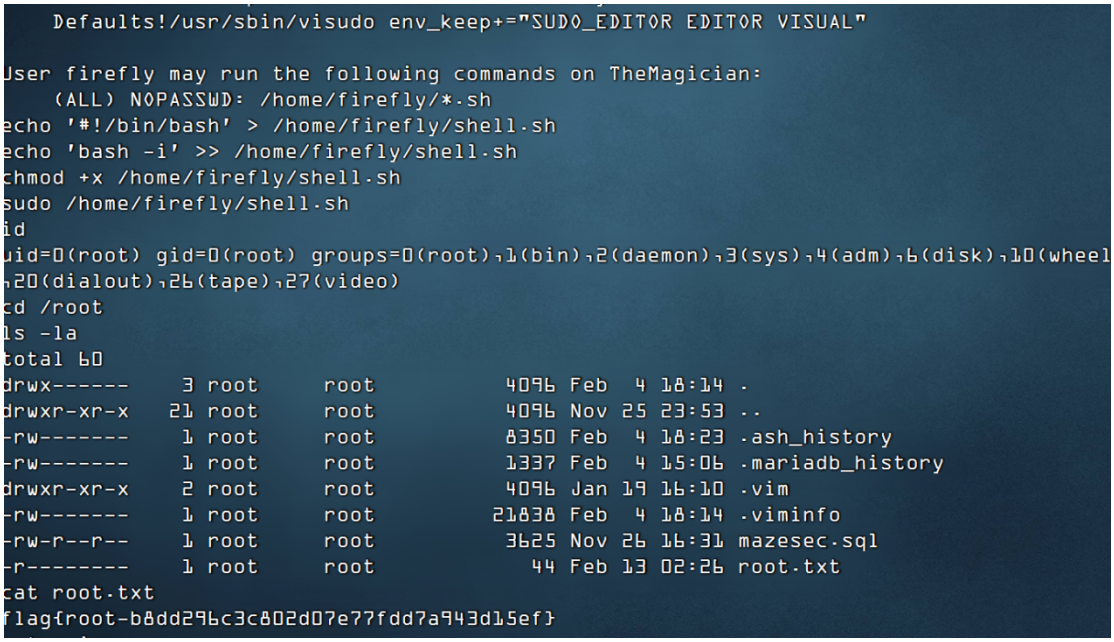
5)写入脚本

我们去 sudo -l ，我们可以看到任何用户都可以无密码去执行

/home/firefly/目录下以 sh 为后缀名的脚本



那么我们就新建一个脚本，写入提权命令，然后去执行即可



我们可以看到成功获取 root 权限，我们去查看 root.txt 即可。