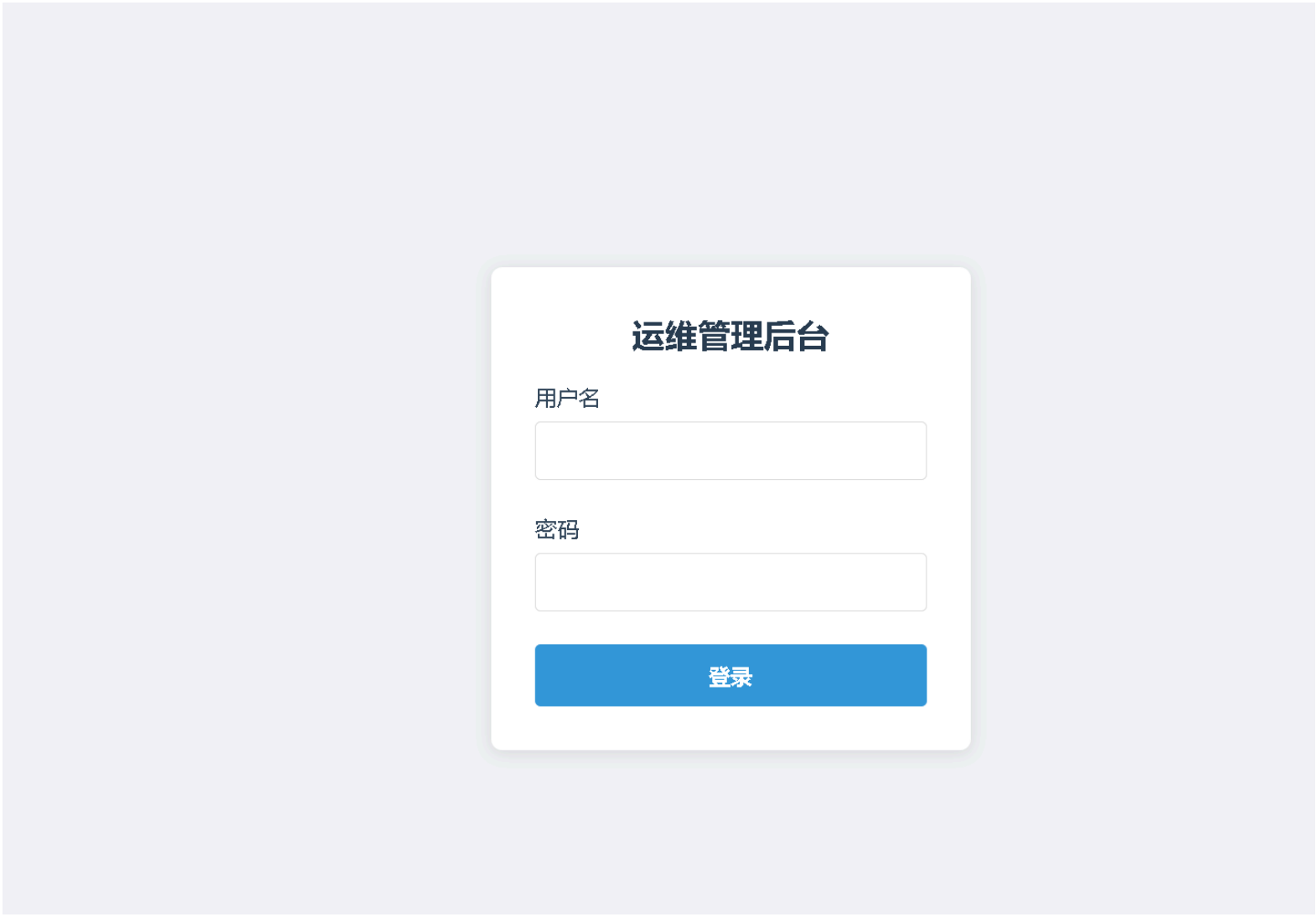
pane l

信息收集

```
nmap -p- 192.168.31.98
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-12 14:04 CST
Nmap scan report for Pane1 (192.168.31.98)
Host is up (0.0012s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
38415/tcp open  unknown
MAC Address: 08:00:27:BE:56:7B (Oracle VirtualBox virtual NIC)
```

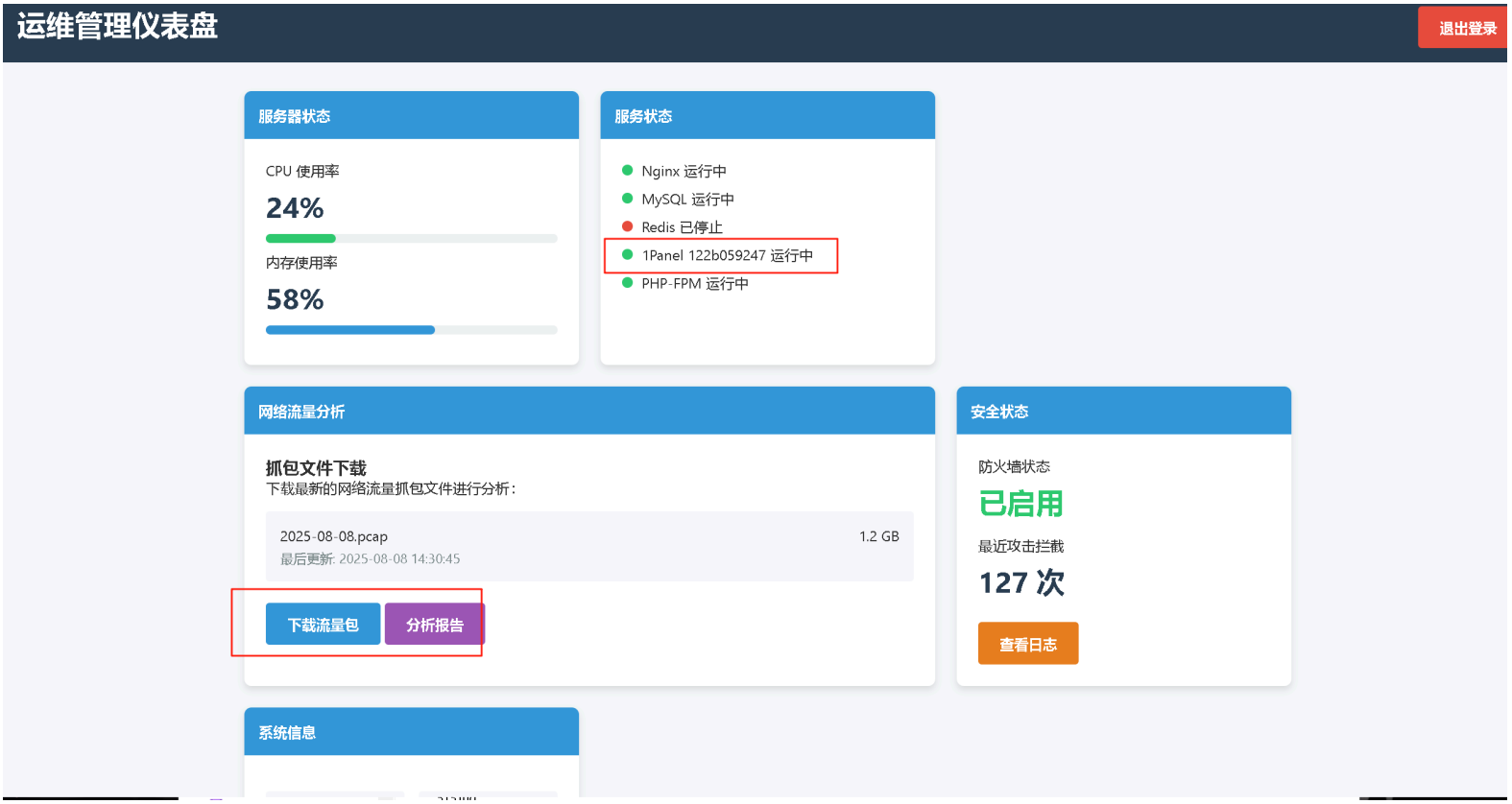
```
irsearch -u http://192.168.31.192
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /root/Desktop/poc/reports/http_192.168.31.192/_25-08-12_16-03-49.txt

Target: http://192.168.31.192/

[16:03:49] Starting:
[16:03:50] 403 -  279B  - /.ht_wsr.txt
[16:03:50] 403 -  279B  - /.htaccess.bak1
[16:03:50] 403 -  279B  - /.htaccess.orig
[16:03:50] 403 -  279B  - /.htaccess.sample
[16:03:50] 403 -  279B  - /.htaccess.save
[16:03:50] 403 -  279B  - /.htaccess_extra
[16:03:50] 403 -  279B  - /.htaccessOLD
[16:03:50] 403 -  279B  - /.htaccessBAK
[16:03:50] 403 -  279B  - /.htaccessOLD2
[16:03:50] 403 -  279B  - /.htaccess_orig
[16:03:50] 403 -  279B  - /.htaccess_sc
[16:03:50] 403 -  279B  - /.htm
[16:03:50] 403 -  279B  - /.html
[16:03:50] 403 -  279B  - /.htpasswd_test
[16:03:50] 403 -  279B  - /.htpasswds
[16:03:50] 403 -  279B  - /.httr-oauth
[16:03:51] 403 -  279B  - /.php
[16:04:30] 302 -    0B  - /dashboard.php  ->  index.php
[16:04:53] 302 -    0B  - /logout.php  ->  index.php
[16:05:17] 403 -  279B  - /server-status
[16:05:17] 403 -  279B  - /server-status/
```

80端口



经过尝试发现administrator 任意密码都可以进入

发现信息1Panel 122b059247 运行中
和流量包



下载流量包得到密码

加上流量包得到密码

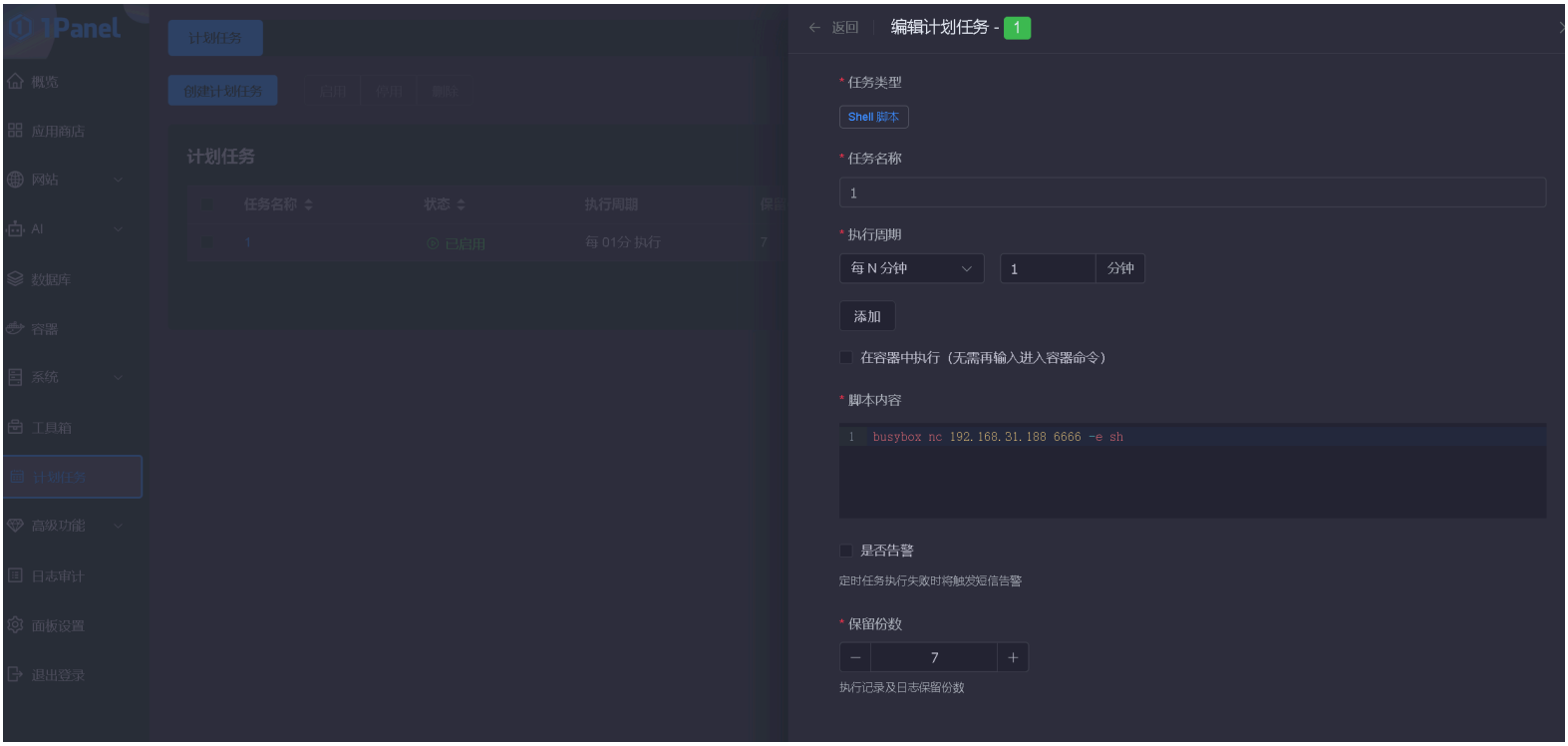
```
[+] 关键字【PASS】【包序号：370】username=admin&password=admin

[+] 关键字【PASS】【包序号：836】username=root&password=superpassword123

[+] 关键字【PASS】【包序号：1677】username=admin&password=superpassword123
```

38415端口

http://192.168.31.192:38415/
一开始爆破了目录没有发现有用的
结合一开始的信息 1Panel 122b059247 运行中
尝试进入

使用流量包的密码root superpassword123

在计划任务里弹 shell



进入后就直接root用户了

```
root@Pane1:/opt/1panel/task/shell/1# ls
20250812032904.log
root@Pane1:/opt/1panel/task/shell/1# cat /root/root.txt
flag{root-e07910a06a086c83ba41827aa00b26ed}
root@Pane1:/opt/1panel/task/shell/1# cat /home/kaada/user.txt
```

```
flag{user-ef68ba312de0daa3dd200a3f9275a6f6}
```