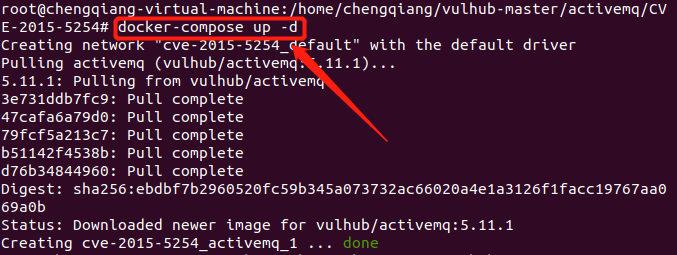
**一、环境搭建**

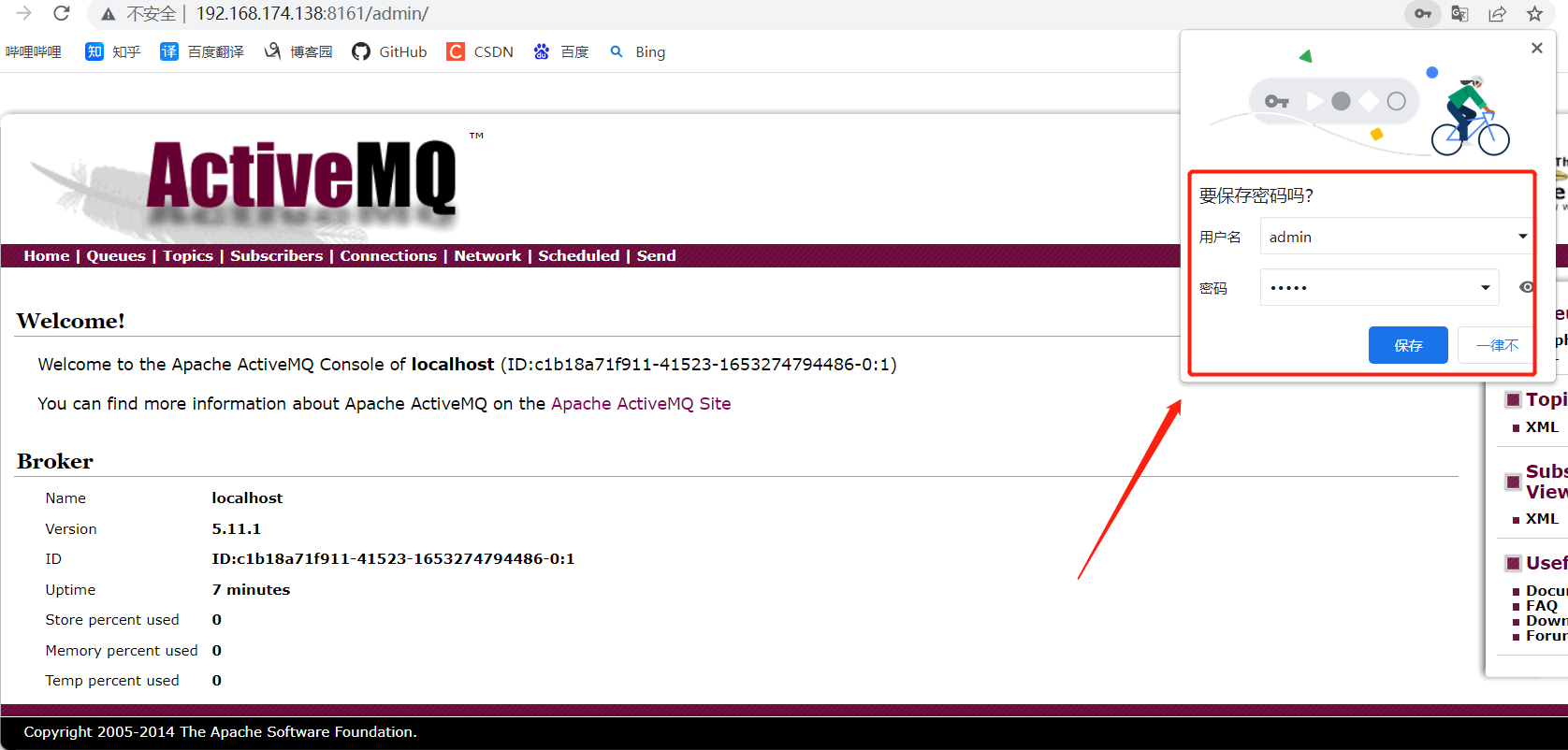
1、Vulhub启动



2、访问8161端口

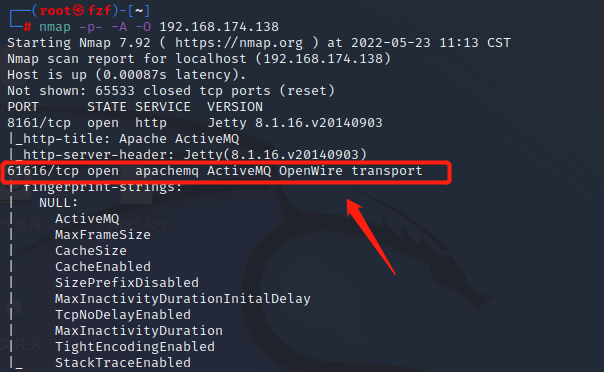


3、管理员默认密码amdin/admin登录



**二、漏洞复现**

1、使用Nmap扫描目标靶机开启的端口，发现目标开启的61616端口上承载这apachemq ActiveMQ服务

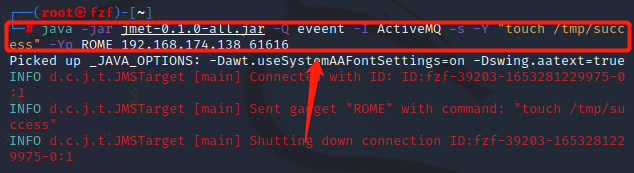


2、在kali攻击机上下载jmet的jar包，然后在同目录下创建external文件夹

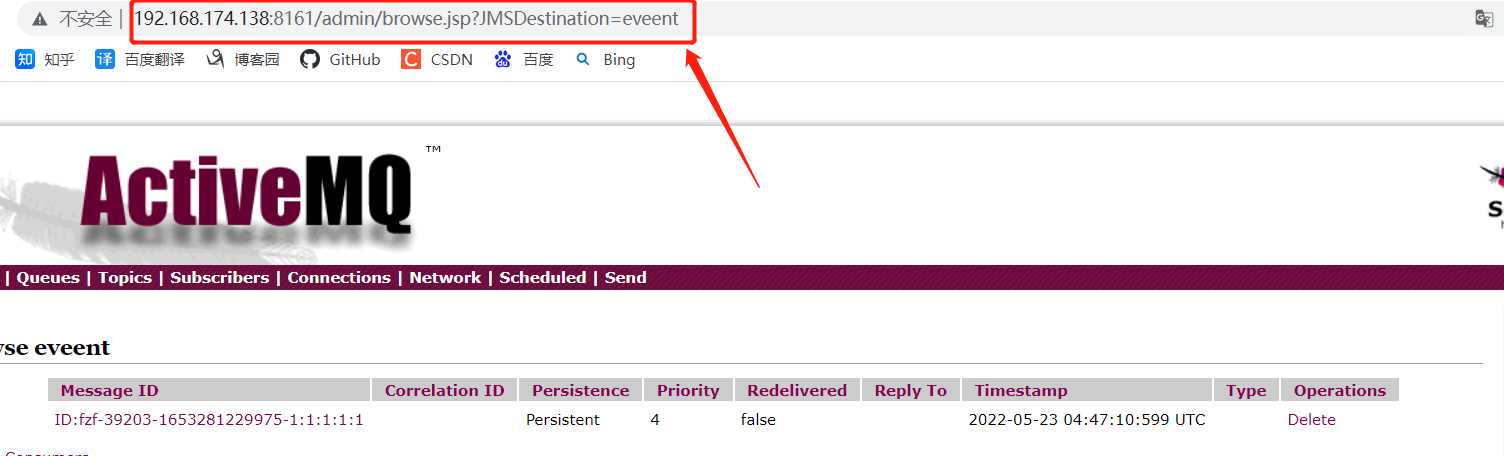
C:\Users\Toby\AppData\Local\Temp\1653283210(1).jpg

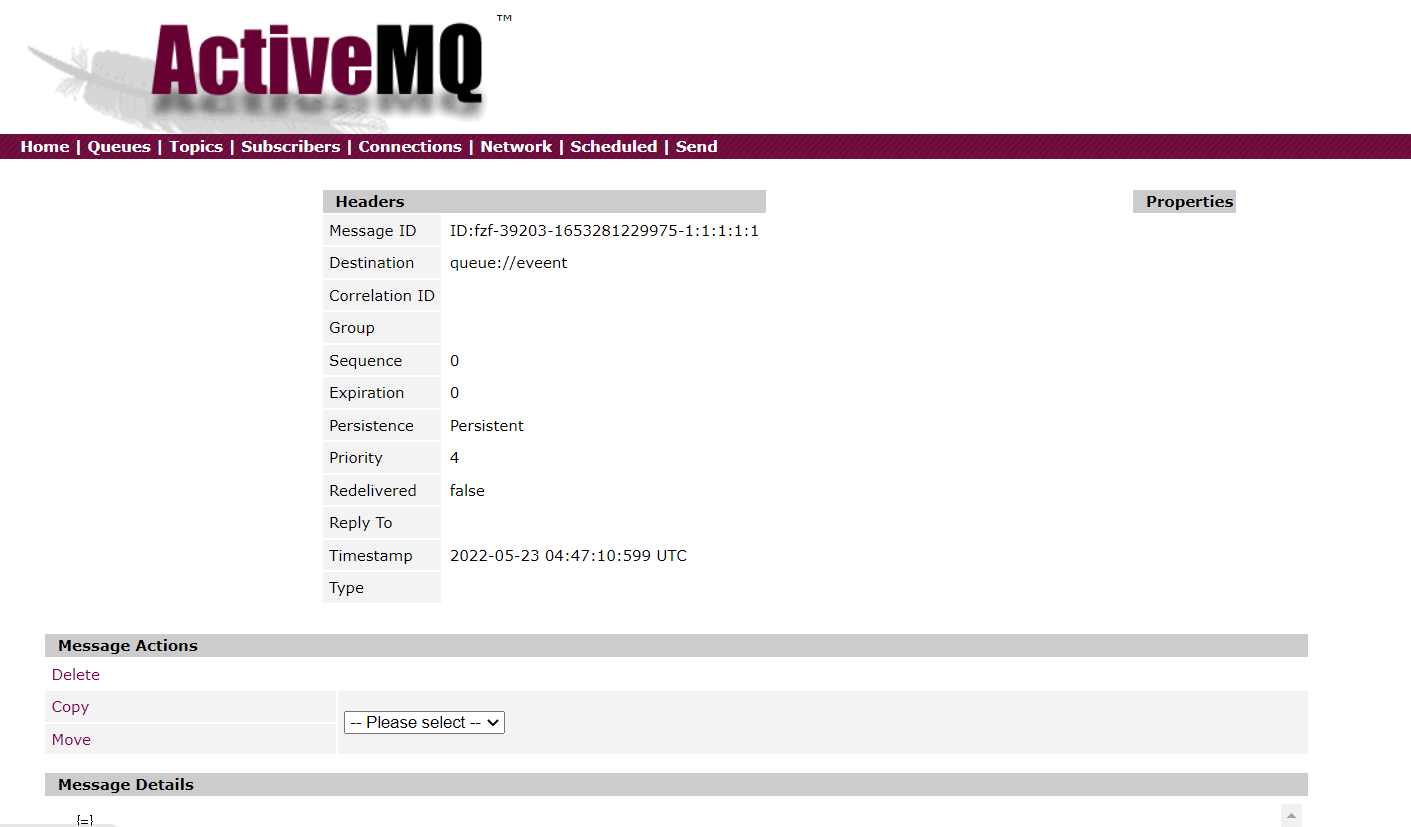
C:\Users\Toby\AppData\Local\Temp\1653283210(2).jpg

3、执行命令，将Payload发送到目标IP的61616端口

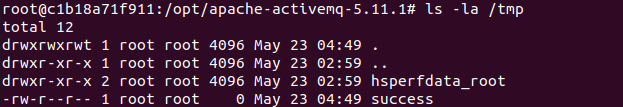
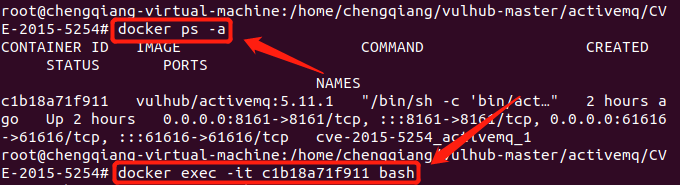


4、此时访问http://192.168.174.138/admin/browse.jsp? JMSDestination=eveent可以查看到所有队列消息。且目标ActiveMQ成功添加一个event列，当他人点击查看这条消息即触发命令执行





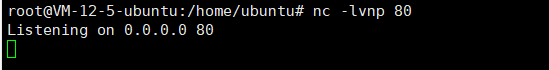
5、登录靶机ActiveMQ容器环境，查看命令执行成功，靶机中/tmp/success文件已创建



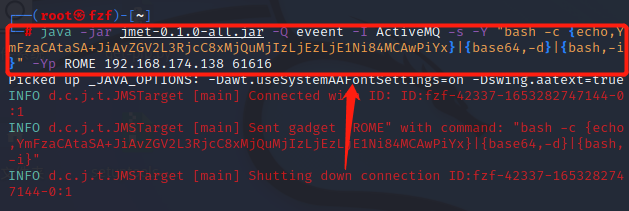
6、编写接下来要执行的命令



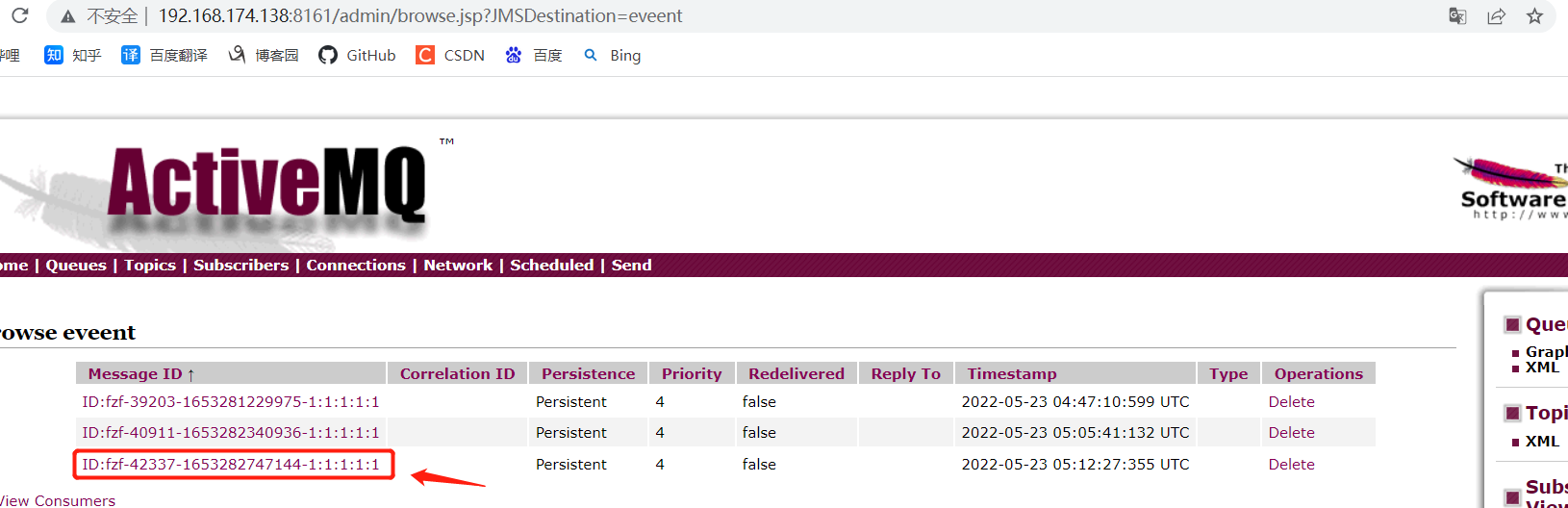
7、VPS开启端口监听



8、Kali执行反弹Shell命令



9、返回之前的even队列，再次点击触发，ID同最后命令执行完的ID一样



10、VPS上成功接收弹回的Shell

