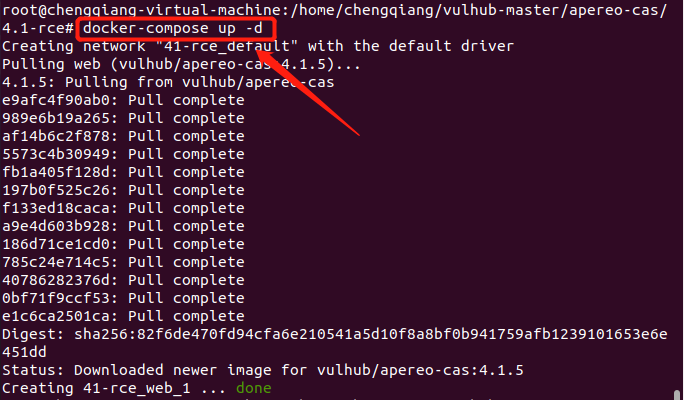
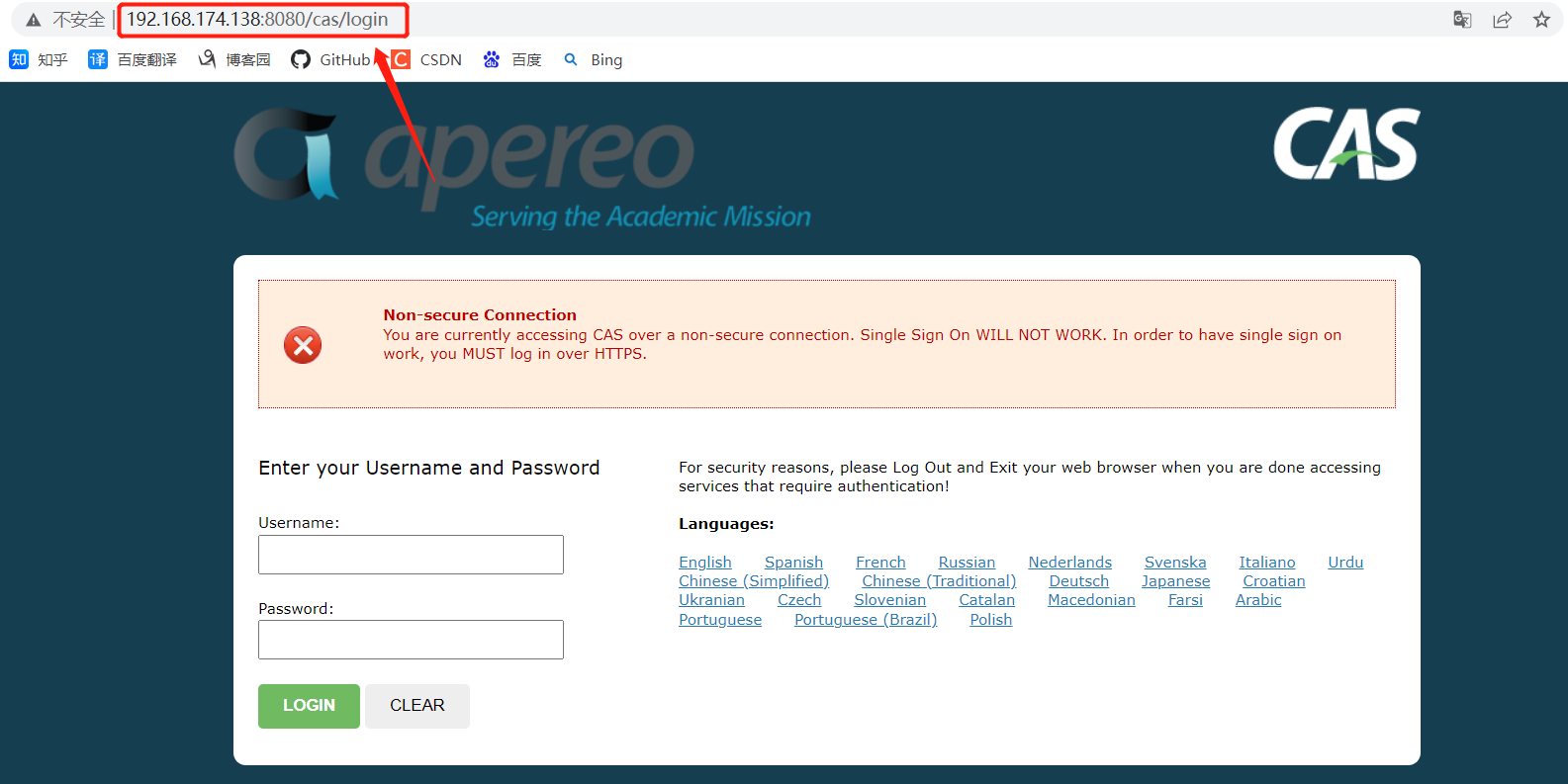
**一、靶场搭建**

1、Vulhub启动



2、访问8080端口下的/cas/login目录

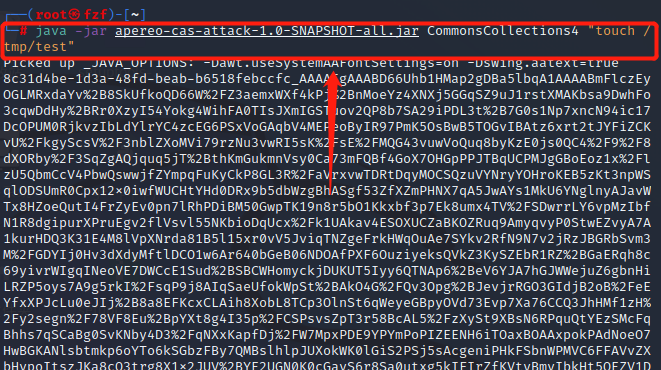


**二、漏洞复现**

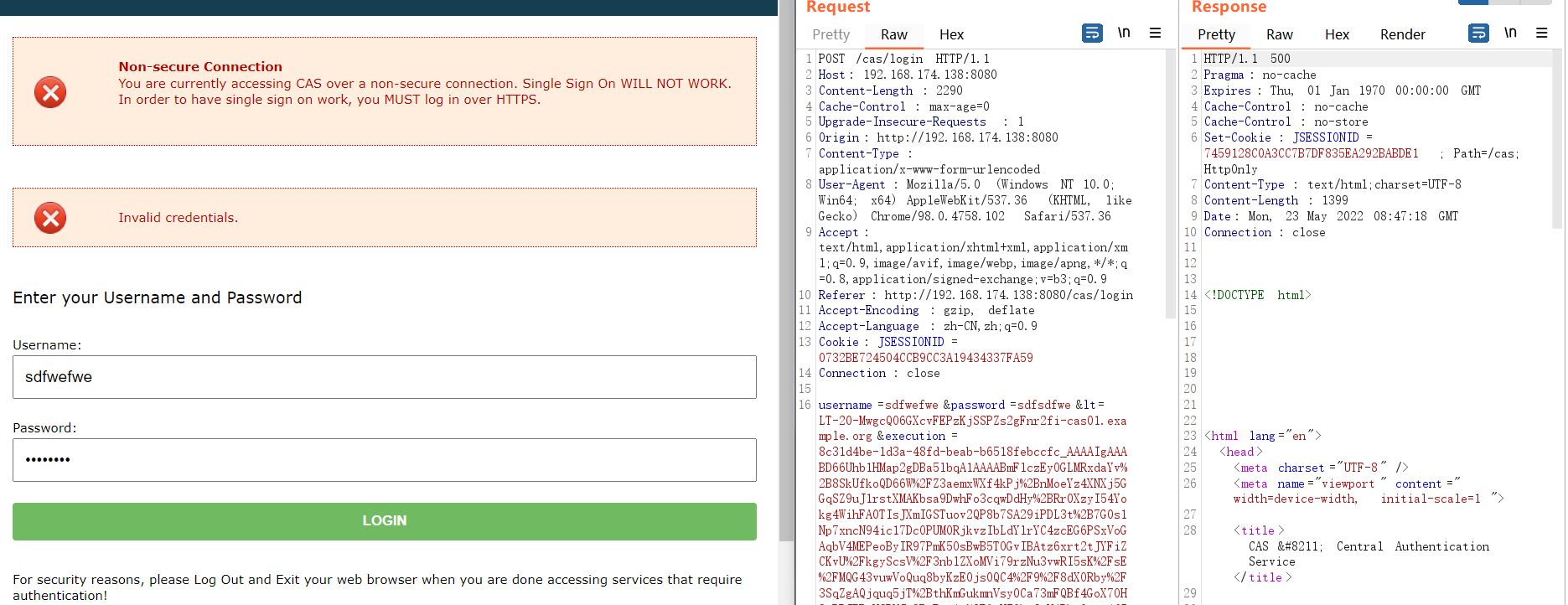
1、下载Apereo-CAS-Attack工具

C:\Users\Toby\AppData\Local\Temp\1653296503(2).jpg

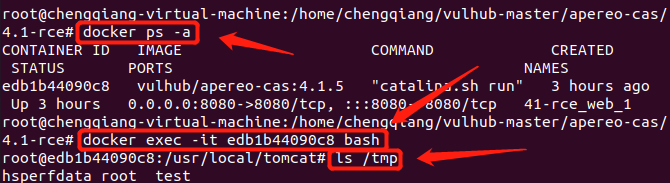
2、生成创建目录的Payload



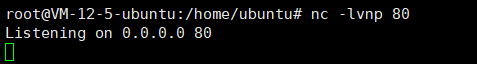
3、访问/cas/login输入任意账号密码并在execution参数中加入Payload



4、登录靶机Docker容器中查看，创建成功



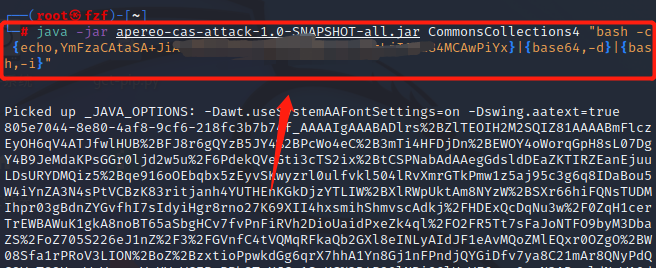
5、VPS开启nc监听端口



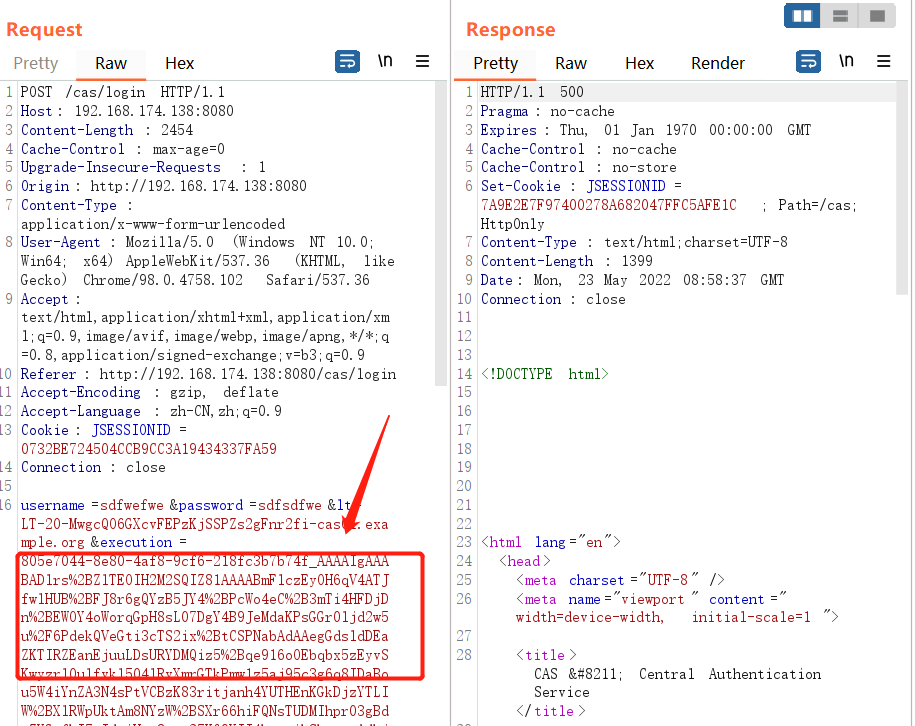
6、编写命令（反弹Shell）



7、生成完整Payload



8、Repeater中添加Payload并重放/cas/login包

9、VPS成功接收返回的Shell

