# Jboss5.X/6.X反序列化漏洞复现

## 1. 漏洞复现

### 环境准备

JBOSS 下载地址：<http://download.jboss.org/jbossas/6.1/jboss-as-distribution-6.1.0.Final.zip>

EXP 下载地址：<https://github.com/yunxu1/jboss-_CVE-2017-12149>

### 环境搭建

**1、下载Jboss环境，并解压**

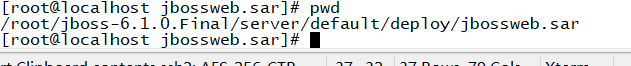
Wget <http://download.jboss.org/jbossas/6.1/jboss-as-distribution-6.1.0.Final.zip>

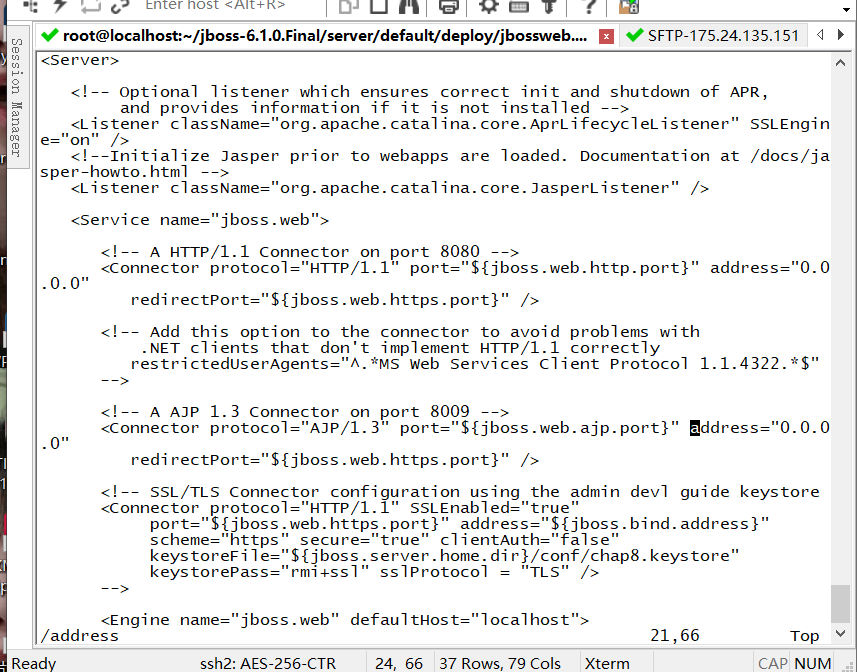
Uzip <http://download.jboss.org/jbossas/6.1/jboss-as-distribution-6.1.0.Final.zip>

**2、修改配置问及那，使网络中的主机都可以访问**

Vim ~/jboss-6.1.0.Final/server/default/deploy/jbossweb.sar/server.xml

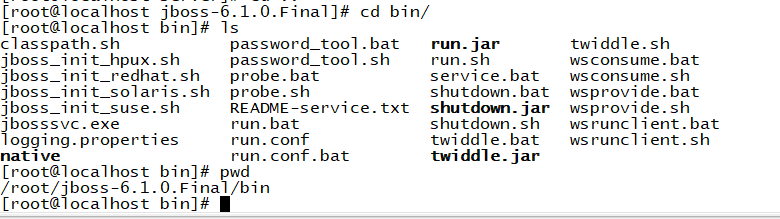
查看当前目录



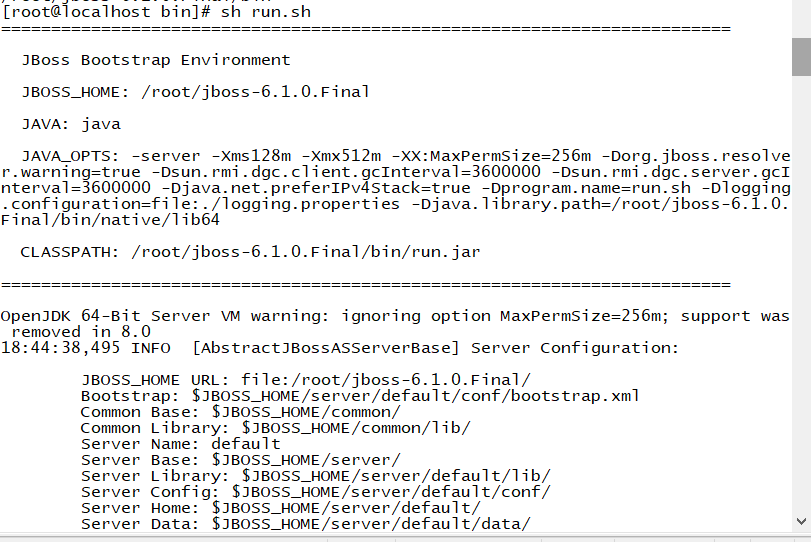


1. 启动Jboss

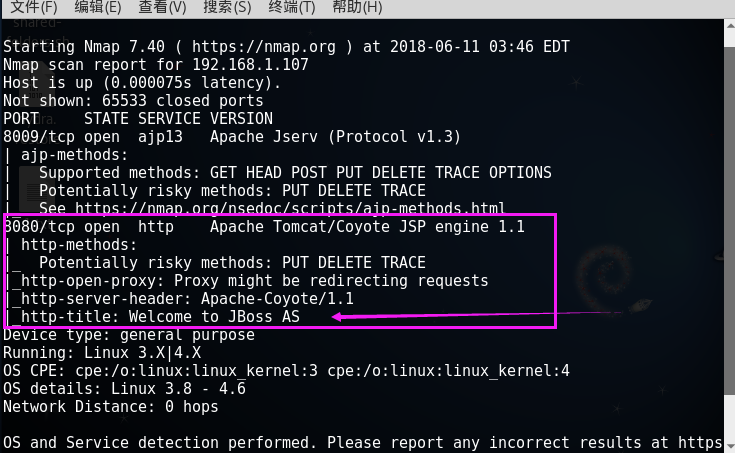
需要在run.sh的目录下进行操作



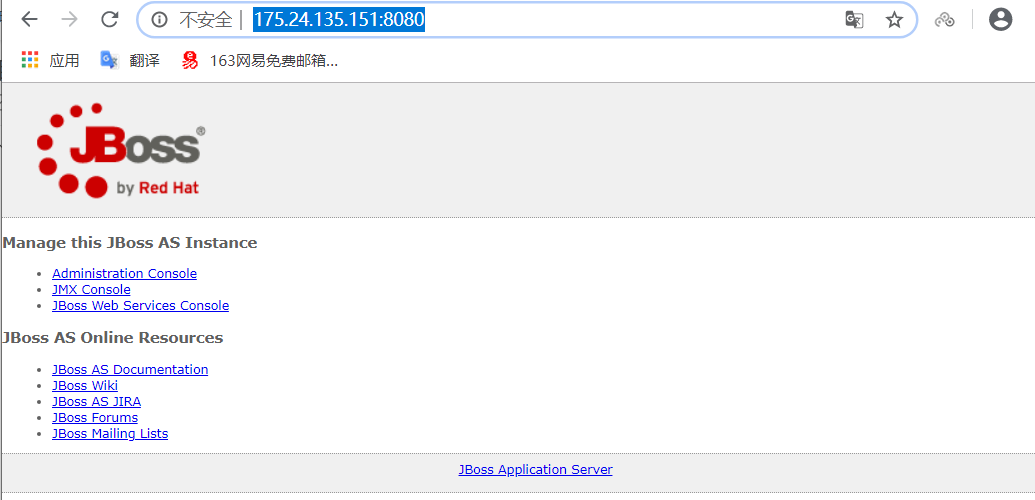
Sh run.sh



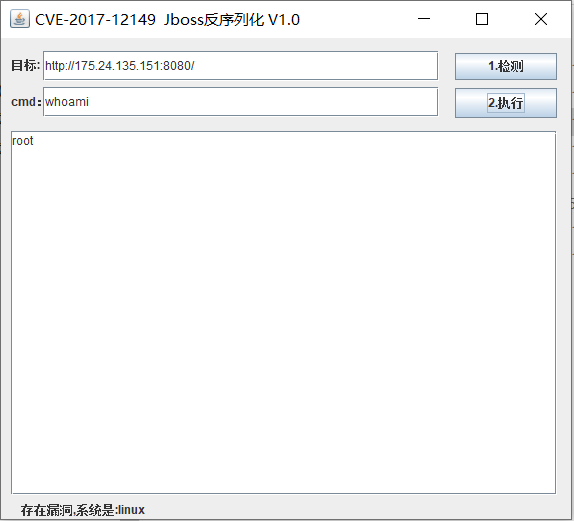
1. 信息收集

利用nmap目标进行扫描

访问目标主机8080端口

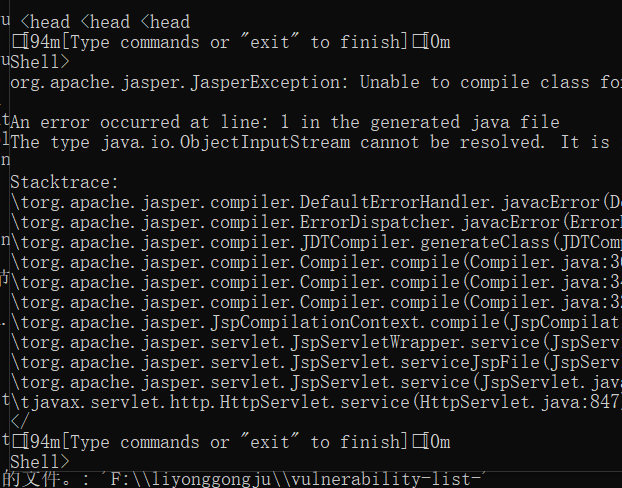


之后下载好EXP利用



或者利用py文件





可以看到shell反弹成功