操作系统

实

验

报

告

**实验名称：\_\_\_\_\_\_\_\_\_实验五\_\_\_ \_\_\_\_\_\_\_**

**小组成员姓名：\_\_\_\_\_\_\_刘俊武\_\_\_\_\_\_\_\_\_\_\_\_\_**

**小组成员学号：\_\_\_SZ160110120\_\_\_\_\_\_\_\_\_\_\_\_**

**学院：\_\_\_\_计算机科学与技术\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**专业：\_\_\_\_\_\_\_\_计算机专业\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

一、实验目的

实验五，的目的主要有以下三点：

1.实践以docker 为新的进程范式的网络访问、会话连接设置、控制及路由

2.通过Wireshark和 Burpsuit等工具进行网络协议分析

3.基于docker的实现机制监控进程行为

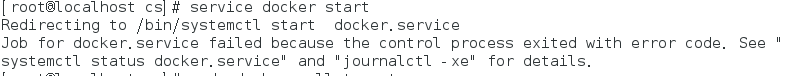
二、实验内容

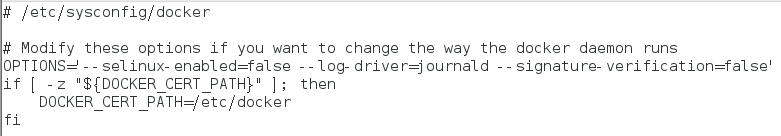
先在centos系统上对docker容器进行部署，再编写登陆和处理页面(login.jsp和action.jsp)。然后通过ssh连接docker容器，使用Wireshark抓包查看抓包信息，使用burpsuite修改数据包，然后观察实验结果。

三、实验过程

1.安装docker

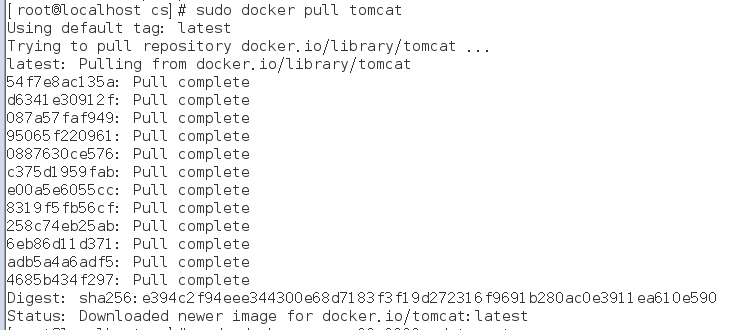
2.启动docker后台服务

3.发现失败了，vi /etc/sysconfig/docker修改docker的配置文件（第一项=false）：

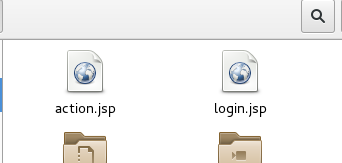
4.然后重新编译并且启动docker后台服务：



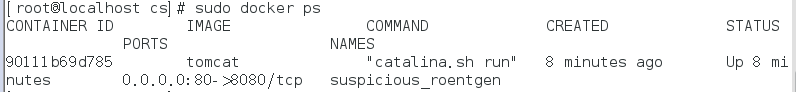
5.在Docker上安装Tomcat工具

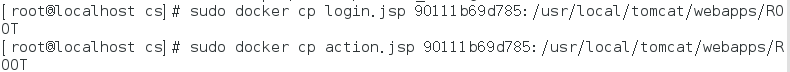
6.安装完毕后，启动Tomcat：

7.先将在物理机上创建的login.jsp和action.jsp文件复制到虚拟机的home中(home代表文件路径)：

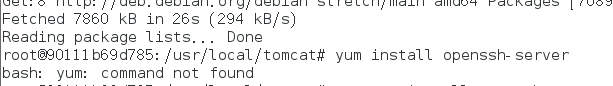


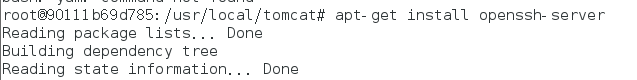
8.获取docker 容器的id：

9.将login.jsp和action.jsp文件docker 容器里：

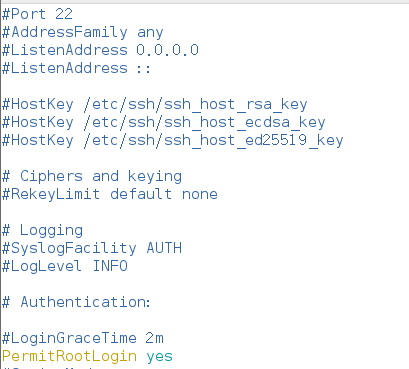
10.通过docker 容器的id 进入正在运行的容器并安装ssh：

11.发现在bash中找不到yum指令，因此需要更新，在更新完后发现还是找不到yum指令，因此我直接使用apt-get install openssh-server安装ssh。

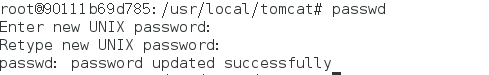




12.安装完vim后，我在进入sshd\_config，将其中的PermitRootLogin 前的#，同时将将值改为yes。

13.启动ssh服务：

14.设置root密码：



15.在新终端上，保存docker容器：

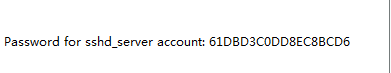
16.在旧的终端上退出，并在新的终端上结束docker：



17.启动刚刚保存的docker并启动ssh服务

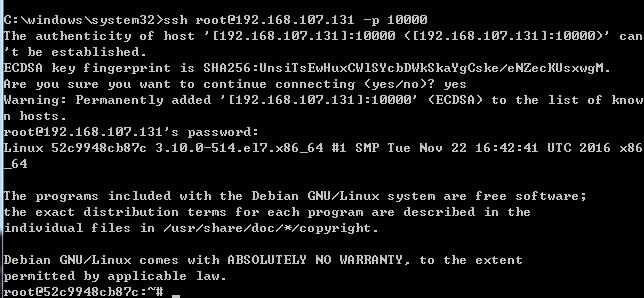
18.查看Linux的IP地址：

19.安装ssh

20.在windows7的cmd窗口中检查是否安装了ssh

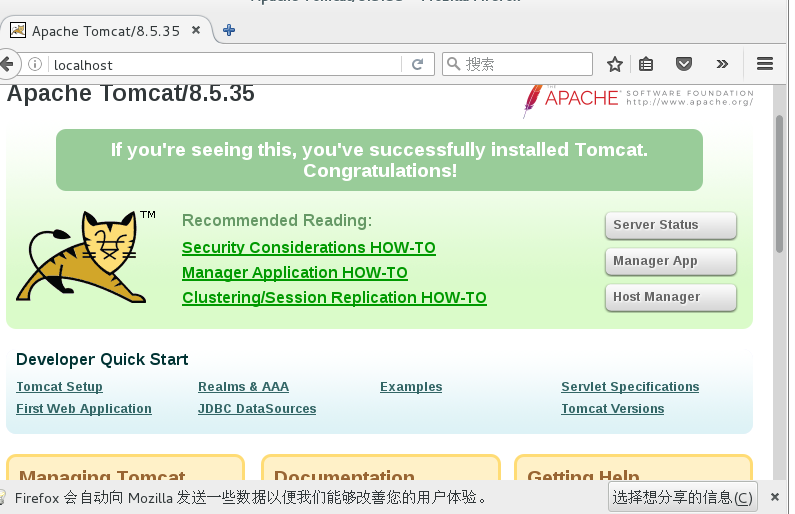


21.在windows7中打开ssh



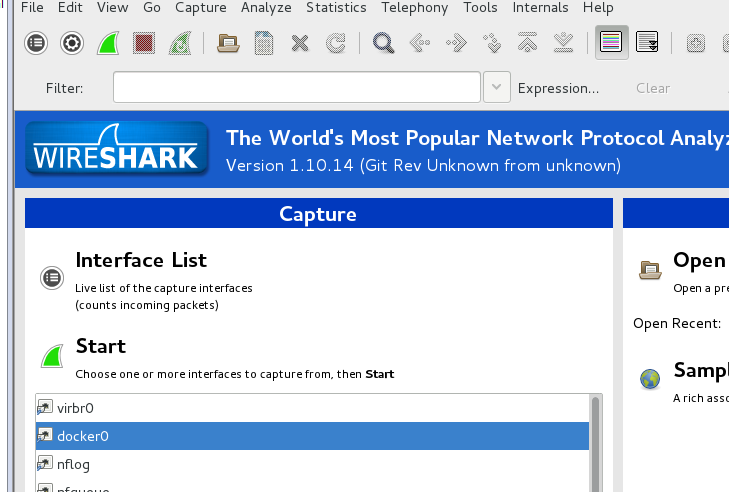
22.在centos中启动Tomcat



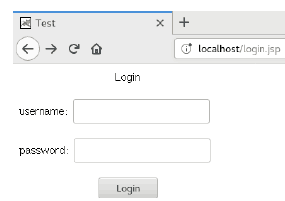
23.在火狐浏览器上访问localhost页面：

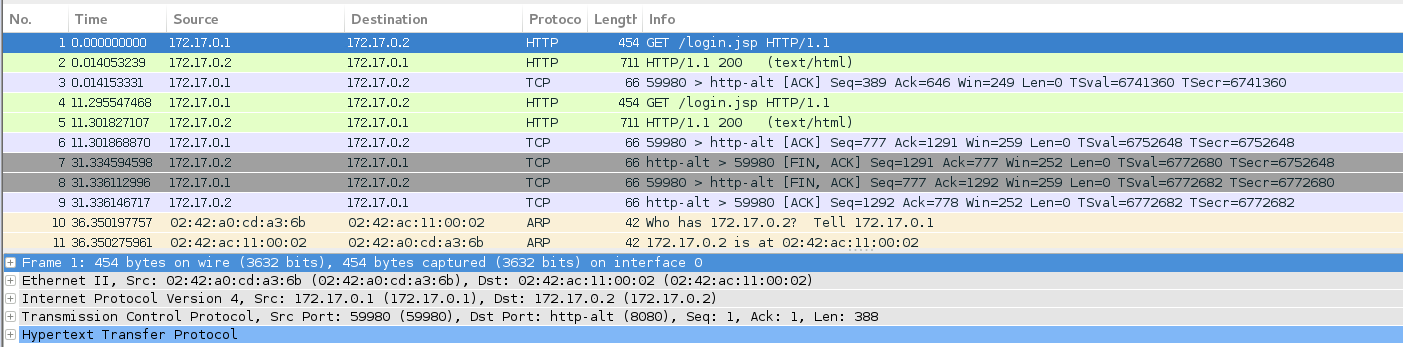
24.安装并启动wireshark：



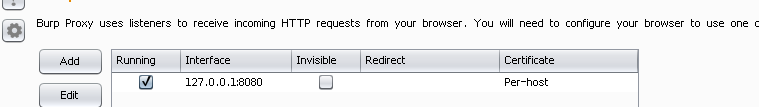
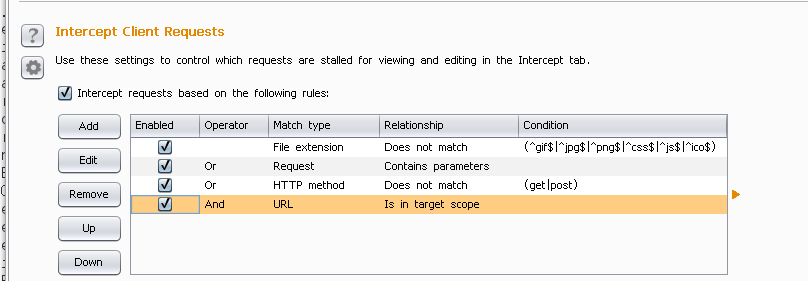
25.选择对docker0进行监测：

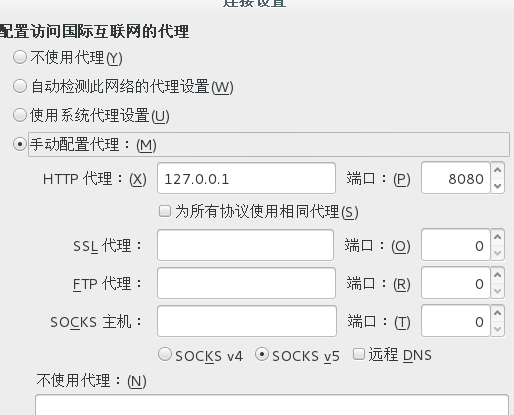
26.在浏览器访问<http://localhost/login.jsp>，的抓包结果

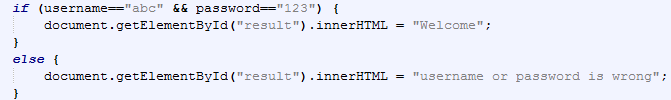


27.在linux中启动burpsuite

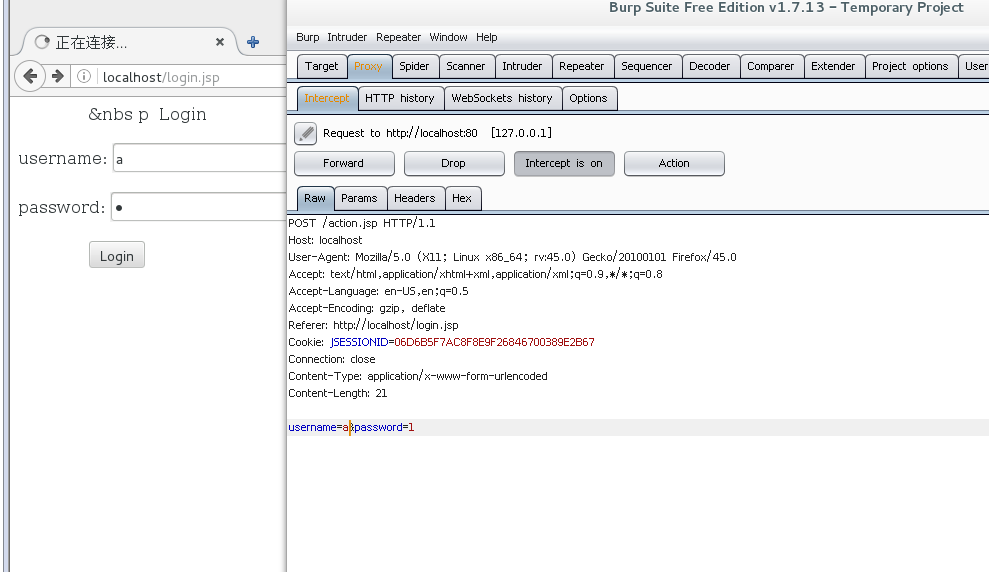
记下Proxy -> Options,记下Proxy Listeners 中的Interface：127.0.0.1:8080

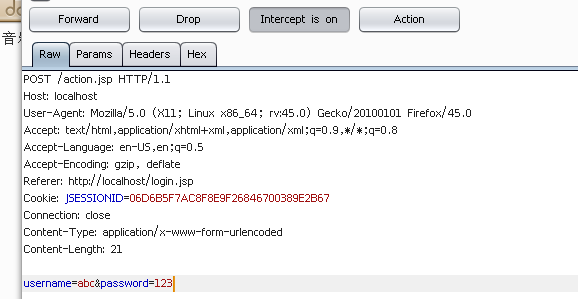
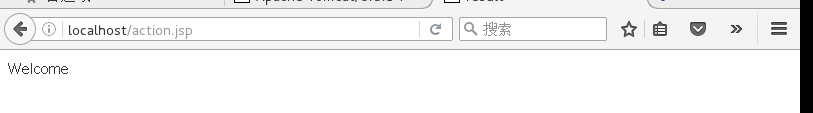
28.设置代理：

29.设置浏览器的代理：

30.进入action.jsp,观测到默认的用户名和密码为“abc”“123”

31.一开始输入用户名a，密码1进行登录，在 burpsuite -> Proxy -> Intercept中，显示抓到的包的内容，发现密码是错误的。

32.在burpsuite中，将，密码改正确后，关闭Intercept，使其变为 ”Intercept is off” ，burpsuite 就会把修改后的包返回给服务器，并且不会再自动抓取服务器发来的包。：

33.登录成功的界面

四、实验结果与分析：

实验结果在上一步呈现出来了，在实验的最后过程中，使用burpsuite开启中断功能后，它会截断浏览器访问网页，并截取传送的数据，在自己修改完传送的数据内容后(将用户名和密码修改为默认的用户名和密码)可以完成登陆。

五、实验课收获与总结

在此次实验中，学会了如何在Linux系统上去完成docker的部署，使用Wreshark进行抓包并进行观察，以及使用burpsuite对截取的数据包进行修改。对在Linux系统上的操作有了更为深刻的理解。

与此同时，我们使用ssh对docker容器进行管理，可以有效防止远程管理过程中的信息泄露问题。

此外，自己不要迷信实验指导书，要敢于质疑，有些复制下来的东西可能有错，譬如login.jsp文件的文件中就有错误，导致我在输入正确的用户名和密码后，不能进入到登陆成功的界面。