# 通过开启docker2375端口实现docker Remote API未授权访问漏洞

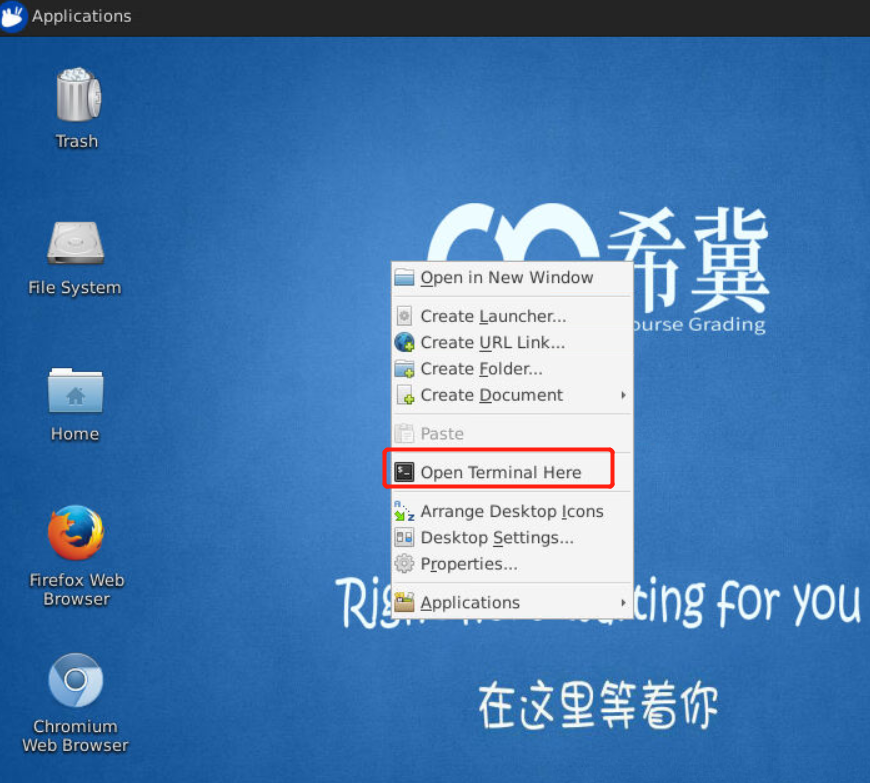
## 1.实验介绍

docker是一个开源的应用容器引擎，允许开发者将其应用和依赖包打包到一个可移植的容器中，并发布到任何流行的Linux机器上，以实现虚拟化。 docker 的 Remote API 因配置不当可以未经授权进行访问，从而被攻击者恶意利用。攻击者无需认证即可访问到docker数据，可能导致敏感信息泄露，黑客也可以恶意删除 docker 上的数据；攻击者可进一步利用 docker 自身特性，直接访问宿主机上的敏感信息，或对敏感文件进行修改，最终完全控制服务器。

## 2.实验原理

管理的docker 节点上会开放一个TCP端口2375，绑定在0.0.0.0上，http访问会返回 404 page not found ，其实这是 Docker Remote API，可以执行docker命令，比如访问 http://host:2375/containers/json 会返回服务器当前运行的 container列表，和在docker CLI上执行 docker ps的效果一样，其他操作比如创建/删除container，拉取image等操作也都可以通过API调用完成。

## 3.实验准备

在远程桌面点开terminal 

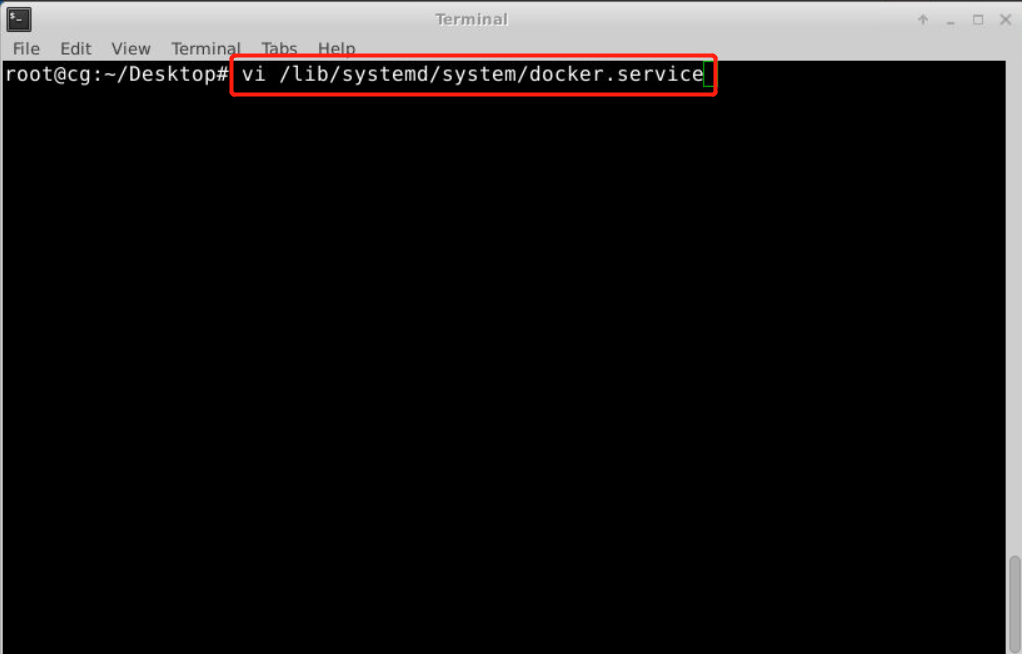
输入以下指令，安装 docker-ce： yum install docker-ce docker-ce-cli containerd.io

## 4.实验步骤

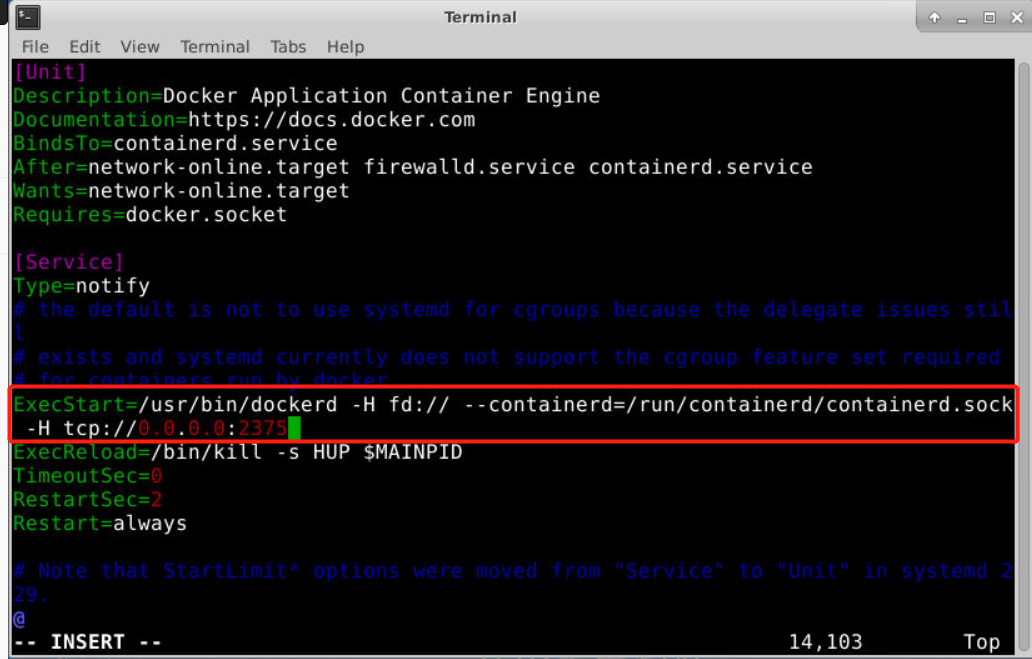
### 1）开放2375端口

修改docker.service配置文件，运行如下命令

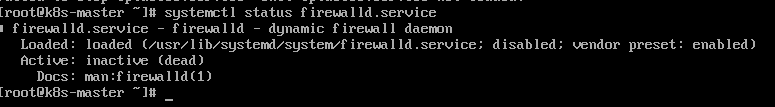
vi /lib/systemd/system/docker.service

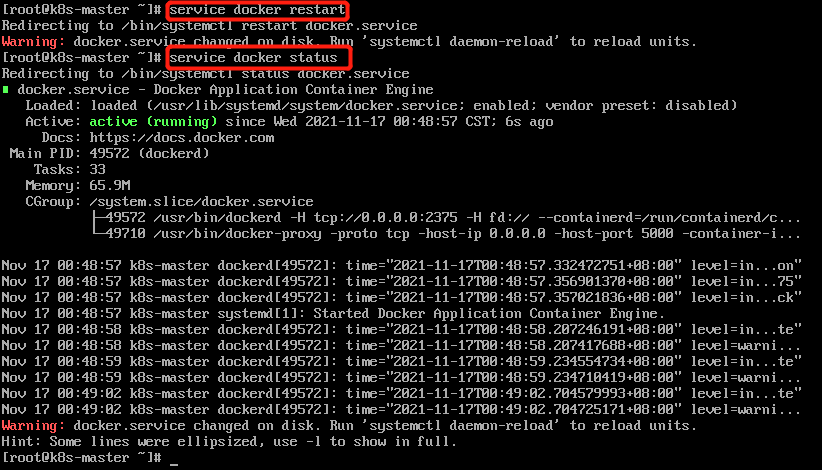


在配置信息中找到“ExecStart”，并在末尾加上-H tcp://0.0.0.0:2375（可点击英文模式下的i/a进入编辑模式，点击“Esc”之后输入“wq”保存）



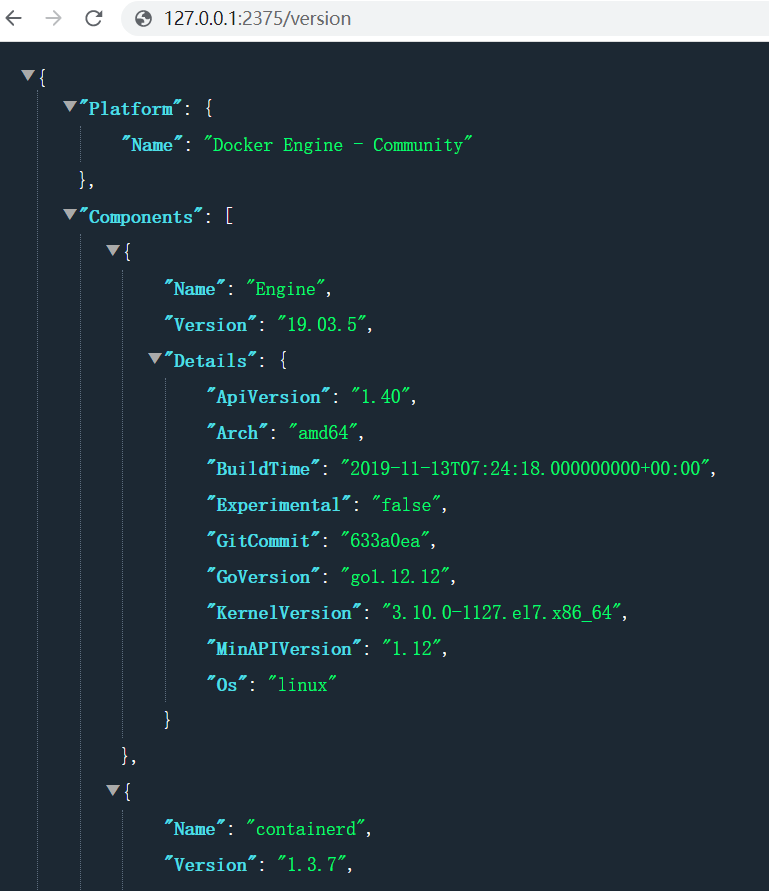
### 2）重启docker服务

这样就设置成功了，然后再检查一下防火墙的的状态 systemctl status firewalld.service 关闭防火墙： systemctl stop firewalld.service 

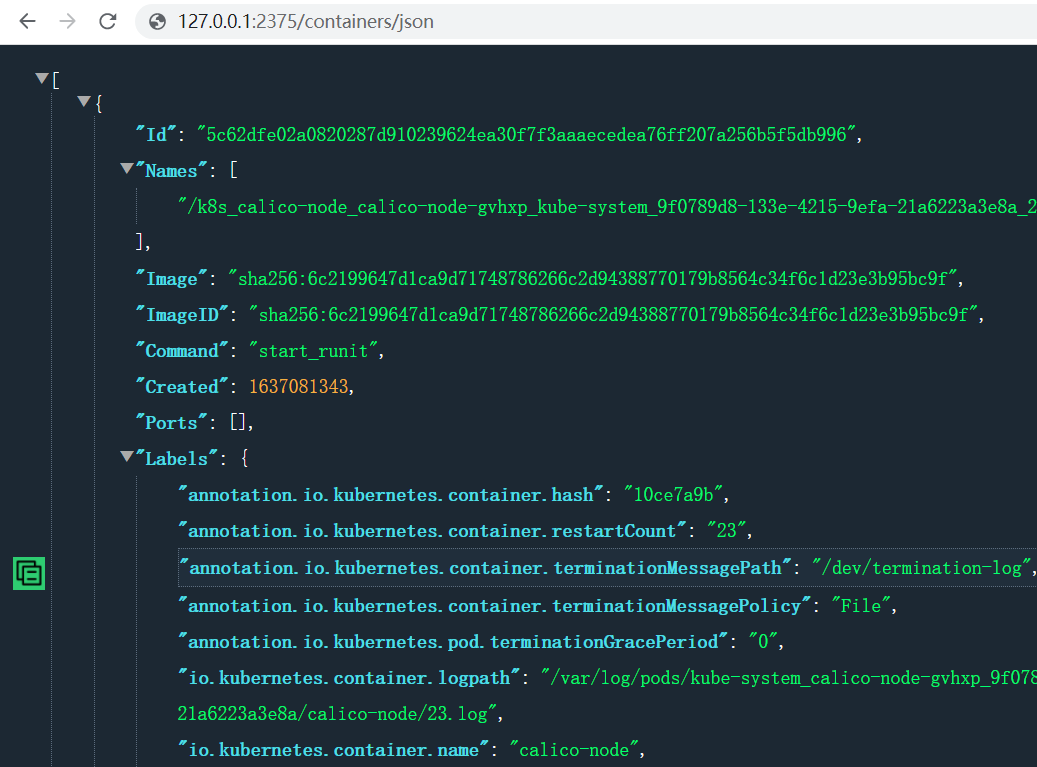
重启docker服务： service docker restart service docker status 

### 3）通过浏览器访问docker api

打开浏览器，输入http://127.0.0.1:2375/version 查看docker版本



输入http://127.0.0.1:2375/containers/json 查看所有运行的docker容器



输入http://127.0.0.1:2375/images/json 查看所有镜像

