## 分析

## ZooKeeper概述

ZooKeeper是一个高性能的分布式数据一致性解决方案，它将复杂的，容易出错的分布式一致性服务封装起来，构成一个高效可靠的原语集，并提供一系列简单易用的接口给客户使用。

* 1. 应用场景：

数据订阅

命名服务：提供名称

* 1. 集群角色：

Leader服务器是整个zookeeper集群工作机制的核心

Follower服务器是zookeeper集群状态的跟随着

Observer服务器充当一个观察者角色

Leader，Follower设计模式

Observer 观察者设计模式

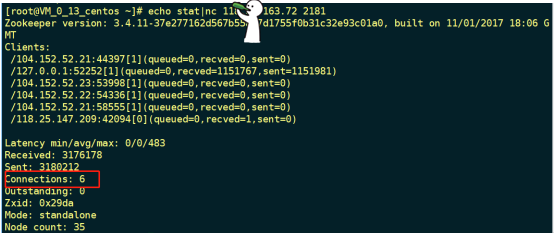
## ZooKeeper未授权访问

ZooKeeper默认开启在2181端口，在未进行任何访问控制情况下，攻击者可通过执行envi命令获得系统大量的敏感信息，包括系统名称、Java环境。

2.1攻击获取信息：

stat：列出关于性能和连接的客户端的统计信息。

echo stat |ncat 127.0.0.1 2181



ruok：测试服务器是否运行在非错误状态。

echo ruok |ncat 127.0.0.1 2181



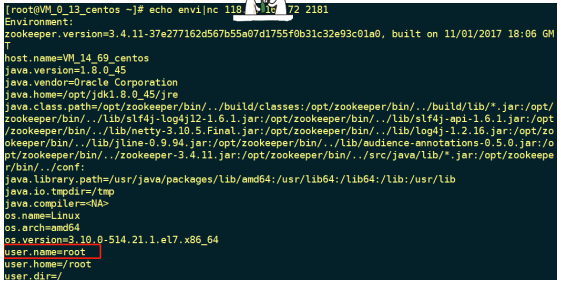
Imok：正常运行

reqs：列出未完成的请求。

echo reqs |ncat 127.0.0.1 2181

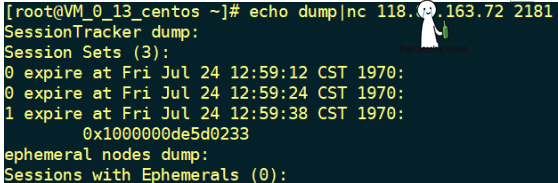
envi：打印有关服务环境的详细信息。

echo envi |ncat 127.0.0.1 2181



dump：列出未完成的会话和临时节点。

echo dump |ncat 127.0.0.1 2181



## 漏洞修复：

禁止把Zookeeper直接暴露在公网

添加访问控制，根据情况选择对应方式（认证用户，用户名密码）

绑定指定IP访问