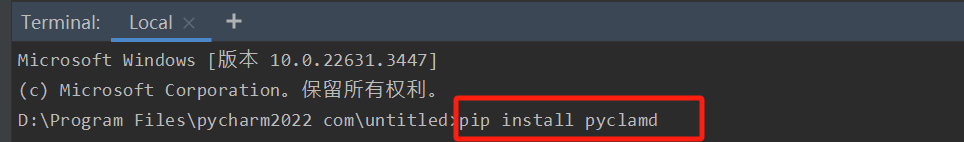
# 一、windows下安装开源clamav杀毒软件

[windows下安装开源clamav杀毒软件 – 六安创世纪网络工程 (hao0564.com)](https://www.hao0564.com/4264.html)

备注：在安装服务时，cmd界面需要以管理员身份运行，不要更改软件的安装路径。

1. **安装pyclamd**



**备注：在安装时需要安装依赖库nose**

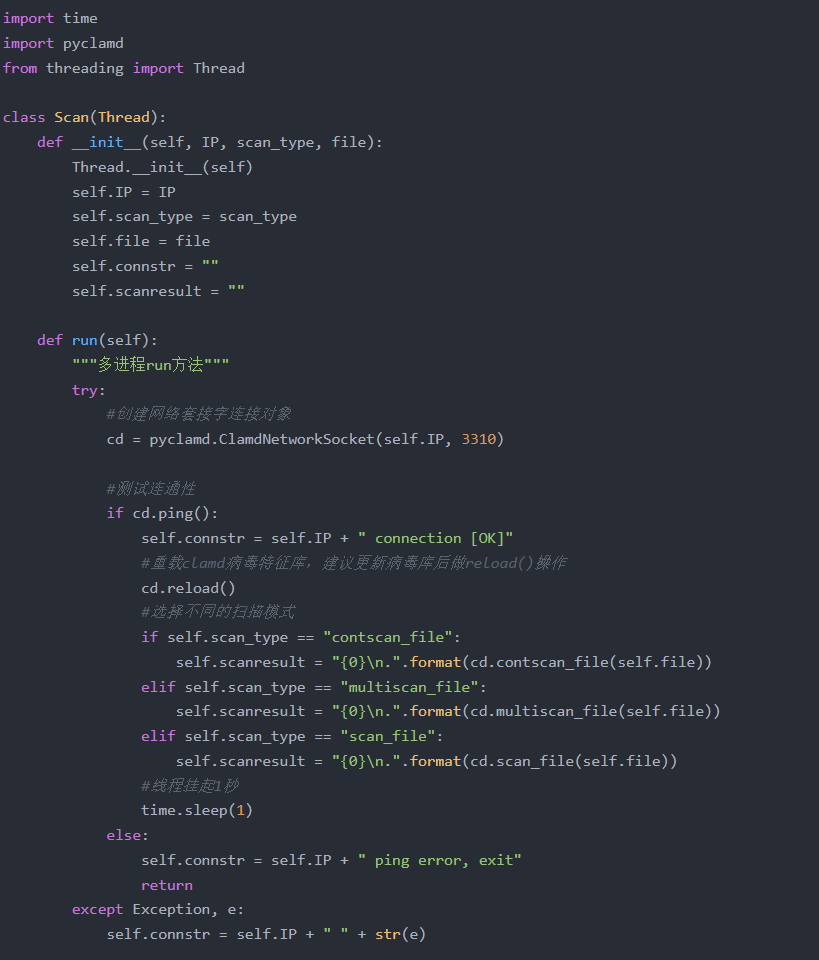
**pip install nose**

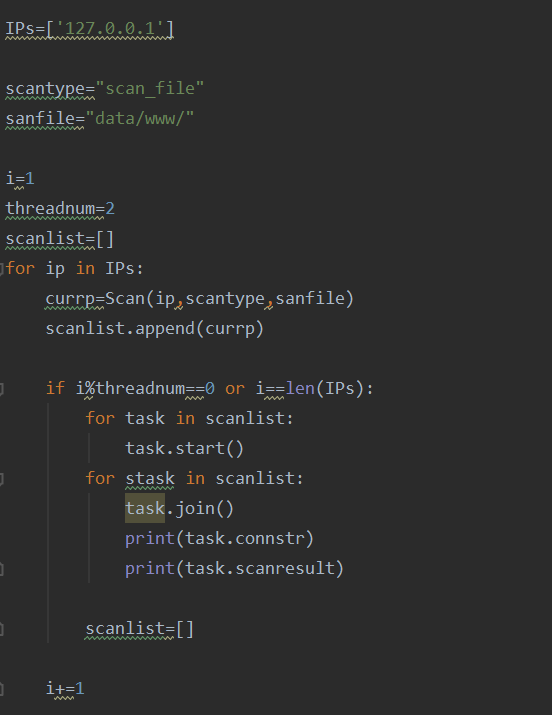
1. **实践：构建集中式病毒扫描系统**

实现了一个集中式的病毒扫描管理，可以针对不同的业务环境定制扫描策略，比如：扫描对象、描述模式、扫描路径、调度频率等。实现的架构如下图，首先业务服务器打开clamd服务(监听3310端口)，管理服务器启用多线程对指定的服务集群进行扫描，扫描模式、扫描路径会传递到clamd，最后返回扫描结果给管理服务器端。



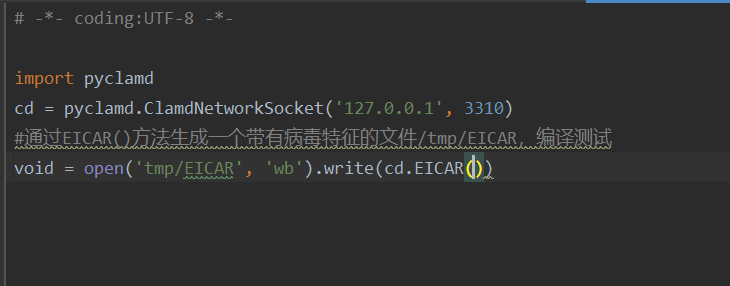
步骤1：通过ClamdNetworkSocket()方法实现与业务服务器建立socket连接，再通过启动不同的扫描方式实施病毒扫描并返回结果，实现的扫描脚本scanner.py代码如下：



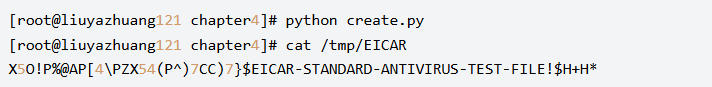


步骤2：生成带病毒特征的文件

利用Python的pyclamd生成病毒特征的文件，这里我们新建一个Python脚本create.py，具体代码如下：



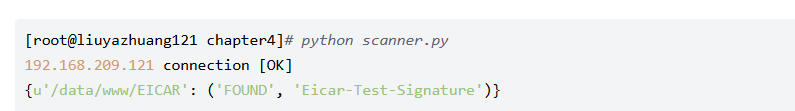
我们运行这个脚本后会在/tmp目录下生成一个EICAR病毒特征文件。



此时，我们将/tmp/EICAR文件移动到/data/www目录下。



步骤3：执行扫描脚本scanner.py，结果如下：



结果显示：发现一个病毒特征文件/data/www/EICAR。