Pipeline between ClamAV and Cuckoo Sandbox

Kết nối giữa ClamAV và Cuckoo Sandbox

1. Mục tiêu

* Tạo ra kết nối giữa 2 ứng dụng ClamAV và Cuckoo Sandbox.
* File cần check sẽ được ClamAV quét và đưa ra kết quả. Nếu ok thì file là file sạch. Nếu kết quả đưa ra khác thì sẽ đẩy file vào Cuckoo Sandbox chạy để lấy log.

1. Chuẩn bị

* Cài đặt ClamAV, Cuckoo Sandbox
* Cài đặt python
* Tài liệu :

+ Clamd : <https://pypi.org/project/clamd/>

+ Cuckoo API : <https://cuckoo.readthedocs.io/en/latest/usage/api/>

1. Thực hiện
   1. Clamd

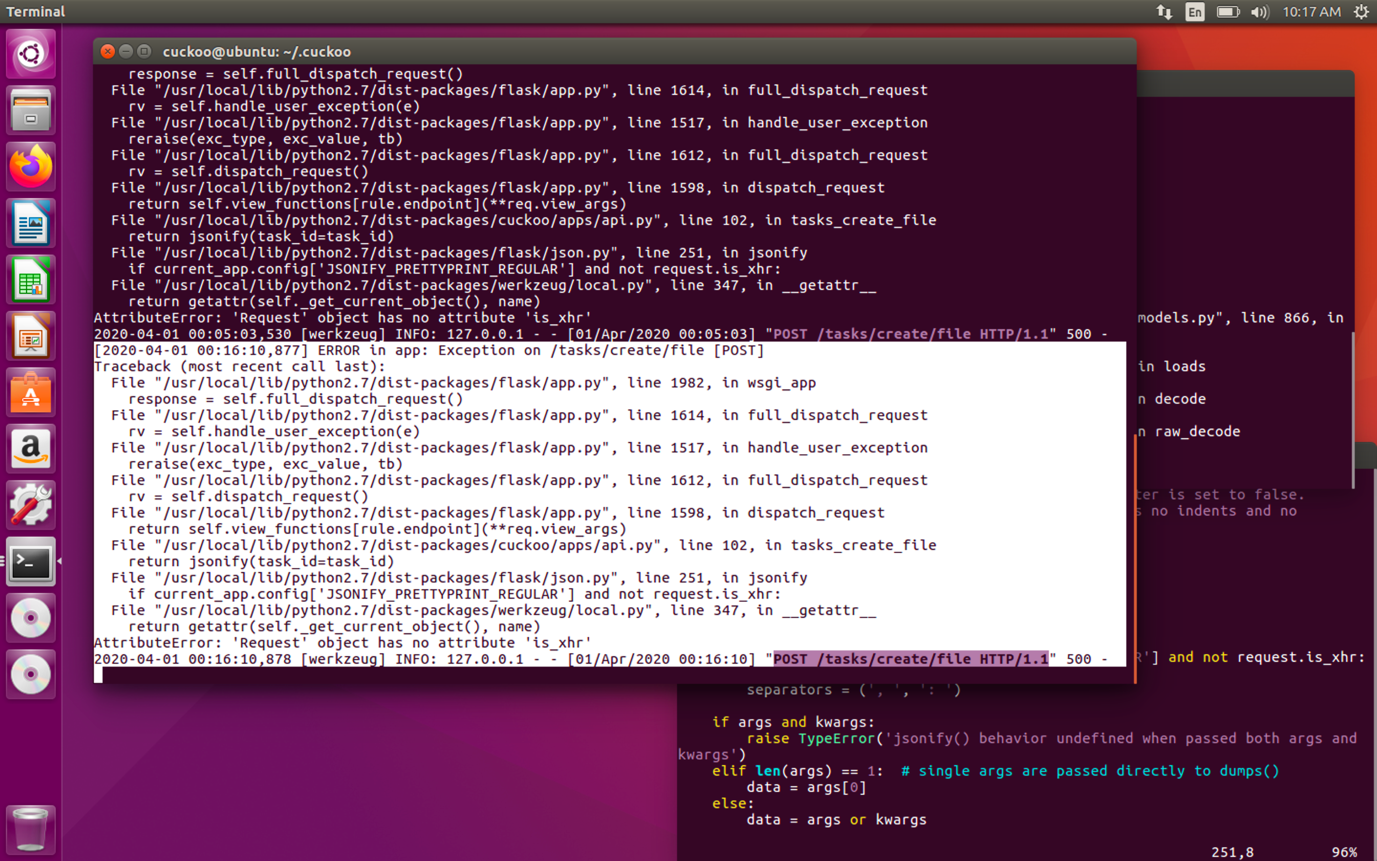
* *clamd* is a portable Python module to use the ClamAV anti-virus engine on Windows, Linux, MacOSX and other platforms. It requires a running instance of the *clamd* daemon.
* Scan file : cd.scan(file)
* Output

Output : {'/tmp/EICAR': ('FOUND', 'Eicar-Test-Signature')}

* Đẩy file sang Cuckoo
  1. Cuckoo
* Khởi động API Server : cuckoo api
* Port mặc định : 8090
* To allow only authenticated access to the API, the api\_token in cuckoo.conf must be set to a secret value. In new Cuckoo installations, a random token is automatically generated for you. To access the API, you must send the Authorization: Bearer <token> header with all your requests using the token defined in the configuration.
* Api\_token đc tạo tự động khi cài cuckoo. Vị trí : $CWD/conf/cuckoo.conf
* Code Sample : <https://github.com/LongLengoc/ClamAVxCuckoo/blob/master/Clamav_Cuckoo.py>

1. Lỗi và cách khắc phục

* Có thể có lỗi sau:



* Chỉnh sửa ở : /usr/local/lib/python2.7/dist-packages/flask/json.py

