# Documentación del Challenge de Programación “Caso Compliance continuo de servidores”

## Contexto

El equipo de Seguridad Informática de Mercado Libre, se encarga de realizar controles sobre el compliance

continuo de distintos servidores en la nube. Por las cantidades de servidores que se administran, poder

asegurar manualmente que estos cumplan el estándar definido por el equipo no es escalable, y se busca

alguna forma de poder alivianar esta tarea.

## Objetivo

Generar un programa (agente) que pueda ser ejecutado en uno de nuestros servidores, y a partir de distintos

comandos del sistema operativo, pueda enviar los siguientes datos a una aplicación (API):

● Información sobre el procesador.

● Listado de procesos corriendo.

● Usuarios con una sesión abierta en el sistema.

● Nombre del sistema operativo.

● Versión del sistema operativo.

Este segundo programa (API) debe consistir en una aplicación con un endpoint que permita al agente enviar

la información relevada, para que luego, sea almacenada en un .csv con el formato:

<IP de servidor>\_<AAAA-MM-DD>.csv

Por lo tanto, el sistema a construir estaría conformado por:

1. Agente - Que será ejecutado en el servidor para recolectar información

2. API - Para centralizar esta información que proviene de los distintos agentes

## Descripción de librerias y funcionamiento del Agente y API

### Librerias y paquetes a instalar:

- pip install flask

- pip install flask-jsonpify

- pip install flask-sqlalchemy

- pip install flask-restful

- pip sqlite3

- apt-get install curl

- apt-get install jq

### Funcionamiento:

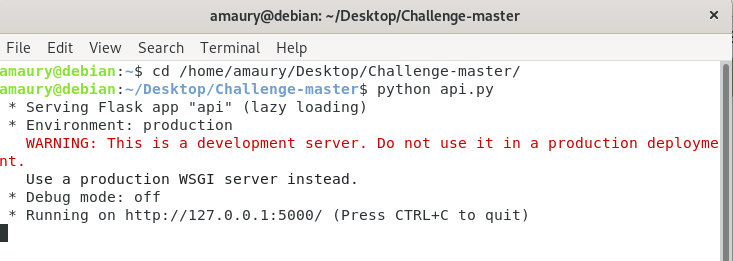
Una vez instaladas las librerias en Debian ya se puede iniciar la API.

API:

1.- Abrir un terminal

2.-Cambiar al directorio donde se encuentra el archivo api.py

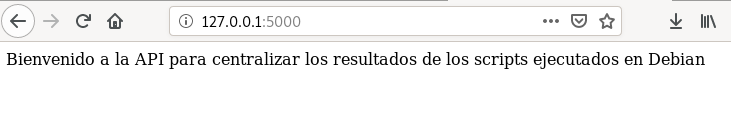
3.-Ingresar “python api.py” y luego presionar “Enter”

La consola indica que la api ya se encuentra corriendo en el Localhost, puerto 5000.

4.- Endpoints

4.1.- Raiz: http://127.0.0.1:5000/

Pantalla de bienvenida a la API



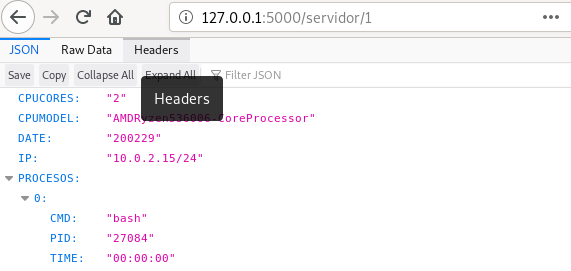
4.2.- Servidores: http://127.0.0.1:5000/servidores

Listado de servidores escaneados desde que se activó la API (Antes de iniciar el agente no habrá resultados)



4.3.- Servidor por ID: http://127.0.0.1:5000/servidor/<ID>

En esta sección se pueden consultar servidores individualmente por ID.



4.4.- Consulta de Servidores registrados en Base de Datos: http://127.0.0.1:5000/bd



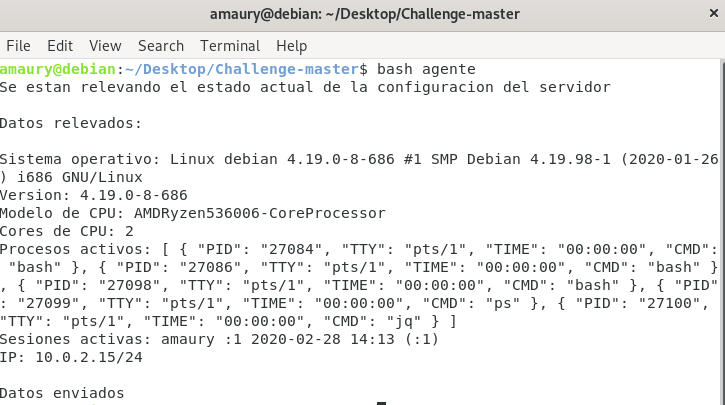
Agente:

1.- Una vez iniciada la API abrir otro terminal

2.-Cambiar al directorio donde se encuentra el archivo “Agente”

3.-Ingresar “bash Agente” y luego presionar “Enter”

4.-El agente se iniciará, ejecutará los comandos para extraer los datos del Sistema Operativo, guardando un archivo temporal en la carpeta /tmp y enviando mediante metodo POST los datos al endpoint de la API.

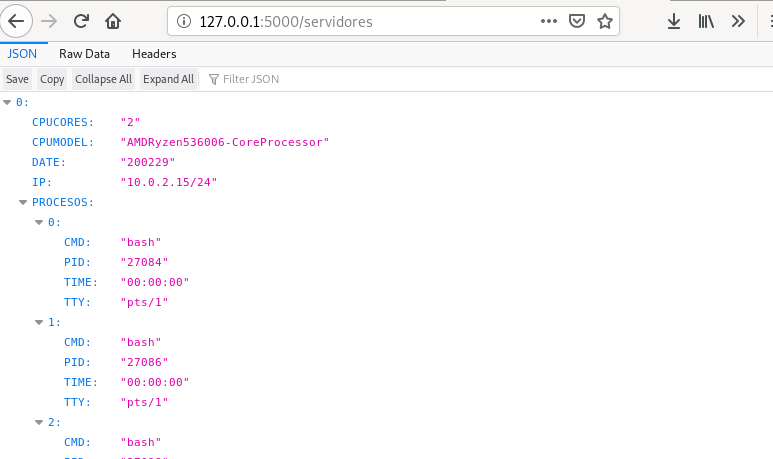


5.-Una vez enviados los datos, el API generará un archivo JSON “<IP>\_<Fecha>.json” en el directorio y creará un nuevo registro en la base de datos “db.db” con el nuevo servidor escaneado, los mismos pueden ser verificados en:

* http://127.0.0.1:5000/bd



* http://127.0.0.1:5000/servidores



* Archivo Json generado

