Guía de Despliegue y Mantenimiento:

Proyecto: Servicio automatizado de alertas de vulnerabilidad CVE (NVD API)

Entorno: Ubuntu 22.04 LTS

Usuario de Ejecución: alertas

Frecuencia: Cada 60 minutos

1. 🛠️ Requisitos e Instalación Inicial

A. Preparación del Sistema

1. Instalar paquetes base (Python y herramientas venv)

sudo apt update

sudo apt install python3 python3-pip python3-venv -y

2. Crear usuario y directorio de producción

sudo useradd -r -s /bin/false alertas

sudo mkdir -p /opt/vuln_alerts/

3. Asignar propiedad al usuario de ejecución

sudo chown -R alertas:alertas /opt/vuln_alerts/

B. Configuración del Entorno Virtual (VENV)

1. Mover archivos a la ubicación final (Asegúrese de que los archivos estén en /home/administrador/ antes de esto)(administrador es el nombre de usuario que tienes)

sudo mv /home/administrador/vuln_alerts.py /opt/vuln_alerts/

sudo mv /home/administrador/config.yaml /opt/vuln_alerts/

sudo mv /home/administrador/requirements.txt /opt/vuln_alerts/

sudo cp /home/administrador/vuln_alerts.service /etc/systemd/system/

sudo cp /home/administrador/vuln_alerts.timer /etc/systemd/system/

2. Crear e instalar dependencias

cd /opt/vuln_alerts/

sudo python3 -m venv venv

sudo /opt/vuln_alerts/venv/bin/pip install -r requirements.txt

#C. Configuración de Rotación de Logs (Logrotate) Para evitar que el archivo de log crezca indefinidamente, configuramos la rotación semanal.

1 sudo nano /etc/logrotate.d/vuln_alerts

2 pegar el siguiente contenido:

```
/opt/vuln_alerts/vuln_alerts.log {
    weekly
    rotate 4
    compress
    delaycompress
    missingok
    notifempty
    create 644 alertas alertas
}
```

---

2. 🤗 Configuración de Credenciales Seguras

A. Crear y Editar el Archivo de Entorno (`/etc/default/vuln_alerts`)

Este archivo inyecta la Contraseña de Aplicación de Office 365 y la lista final de destinatarios.

Nota: Debe sustituir los valores entre corchetes [] por los datos reales de la empresa.(en el archivo de variables de entorno.txt de la carpeta viene)

sudo nano /etc/default/vuln_alerts

Contenido a pegar:

NVD_API_KEY="PON TU NVD API KEY AQUI"

SMTP_HOST="smtp.gmail.com"

SMTP_PORT="587"

SMTP_USER="CORREO DESDE EL QUE ENVIAS LAS ALERTAS"

SMTP_PASS="[CONTRASEÑA DE APLICACIÓN]"

Lista de destinatarios separada por comas

SMTP_FROM="no-reply@empatiza.es"

SMTP_TO="CORREO EN QUE RECIBES LAS ALERTAS"

Restringir Permisos (CRÍTICO para la seguridad)

sudo chmod 600 /etc/default/vuln_alerts

---

3. ⚙️ Activación Final del Servicio

Esta secuencia inicia el servicio (`vuln_alerts.service`) cada 30 minutos, gestionado por el temporizador (`vuln_alerts.timer`).

1. Recargar Systemd (para leer las nuevas unidades y el EnvironmentFile)

sudo systemctl daemon-reload

2. Habilitar el temporizador (para que persista en reinicios)

sudo systemctl enable vuln_alerts.timer

3. Iniciar el temporizador inmediatamente

sudo systemctl start vuln_alerts.timer

4. Verificar el estado (Comprobar 'Active: active (waiting)' y 'Trigger:')

sudo systemctl status vuln_alerts.timer

4. 🔍 Verificación y Diagnóstico

A. Ejecución de Prueba Inmediata (Envío de Correo)

Si necesita forzar una ejecución para comprobar que el correo sal

Borra la DB (para reenviar alertas) y ejecuta el servicio una vez

sudo rm -f /opt/vuln_alerts/cve_alerts.sqlite

sudo systemctl start vuln_alerts.service

Revisar logs (buscar "Correo enviado exitosamente")

tail -n 20 /opt/vuln_alerts/vuln_alerts.log