GUÍA DE USO – SISTEMA DE ALERTAS DE VULNERABILIDAD (NVD SCANNER)

Este documento ofrece una guía clara y directa para comprender, mantener y modificar el sistema automatizado de monitoreo de vulnerabilidades (CVE) instalado en el servidor Ubuntu. Su objetivo es facilitar el trabajo de cualquier persona que necesite operar, ajustar o auditar el sistema.

FUNCIONALIDAD Y ESTRUCTURA DEL SCRIPT

Componente	Función Principal	Ubicación
vuln_alerts.py	Lógica de consulta (NVD), filtrado (CVSS/Fabricante), prevención de duplicados y envío de correo.	/opt/vuln_alerts/
config.yaml	Contiene la **lista de fabricantes a monitorear** y el umbral de riesgo (CVSS).	/opt/vuln_alerts/
cve_alerts.sqlite	Base de datos que registra CVEs ya notificadas y un log de auditoría (email_log).	/opt/vuln_alerts/
vuln_alerts.timer	Unidad Systemd que programa la ejecución del script cada 30 minutos.	/etc/systemd/system/
/etc/default/vuln_alerts	Archivo seguro que almacena las credenciales SMTP, la API Key y la **lista de destinatarios de correo.**	/etc/default/

MODIFICACIÓN DE FABRICANTES Y UMBRAL DE RIESGO (CVSS)

Tarea	Archivo a Editar	Valores a Modificar
Añadir/Quitar Fabricantes	/opt/vuln_alerts/config.yaml	Modificar la lista bajo **keywords:**. Asegúrese de mantener la indentación (dos espacios y guion).
Modificar Destinatarios	/etc/default/vuln_alerts	Editar la variable SMTP_TO. Separe los correos con comas.
Cambiar Nivel de Riesgo (CVSS)	/opt/vuln_alerts/config.yaml	Modificar **min_score: 4.0**. (4.0 = Medio, 7.0 = Alto, 9.0 = Crítico).

⚠ **Nota:** Tras cambiar esto, debe ejecutar: sudo systemctl restart vuln_alerts.service

COMANDOS DE MANTENIMIENTO Y RECARGA

Tarea	Comando a Ejecutar	Propósito
Aplicar Cambios (Esencial)	sudo systemctl daemon-reload	Fuerza a Systemd a leer las modificaciones en los archivos de configuración.
Verificar Estado	sudo systemctl status vuln_alerts.timer	Muestra cuándo es la próxima ejecución y si el sistema está activo.
Forzar Ejecución (Test)	sudo systemctl start vuln_alerts.service	Ejecuta el script una vez inmediatamente para probar cambios (útil con dry-run).
Revisar Logs Detallados	sudo journalctl -u vuln_alerts.service -r -n 50	Muestra el output y los errores de las últimas ejecuciones (útil para diagnosticar fallos SMTP o de permisos).
Limpiar Histórico (Cuidado)	sudo rm -f /opt/vuln_alerts/cve_alerts.sqlite	Borra la base de datos de CVEs notificadas y el log de email. Usar solo si se desea reenviar todas las alertas históricas.

CAMBIO DE FRECUENCIA DE EJECUCIÓN

Para modificar cada cuánto tiempo se ejecuta el servicio, edite el archivo del temporizador de systemd y cambie el valor de intervalo:

Archivo a editar: /etc/systemd/system/vuln_alerts.timer

Modificar la línea:
   OnUnitActiveSec=60min
por:
   OnUnitActiveSec=180min