Guía de Instalación, Configuración y Validación de GVM/OpenVAS en Kali Linux

> Esta guía detalla cómo instalar, configurar, verificar y acceder a Greenbone Vulnerability Management (GVM) — también conocido como OpenVAS — en Kali Linux, incluyendo el método técnico utilizado para validar el usuario administrador vía línea de comandos.

1. Actualizar el sistema

Antes de instalar cualquier herramienta, asegúrate de tener tu sistema completamente actualizado:

```
sudo apt update && sudo apt upgrade -y
```

2. Instalar Greenbone Vulnerability Management (GVM)

Instala GVM y todos sus componentes integrados:

```
sudo apt install gvm -y
```

Esto instalará:

- `ospd-openvas`: motor de escaneo
- `gvmd`: administrador de escaneos y reportes
- `gsad`: interfaz web
- `gvm-cli`, `gvm-start`, `gvm-check-setup`, entre otros

3. Inicializar GVM por primera vez

Ejecuta el siguiente comando para configurar la base:

sudo gvm-setup

Este paso realiza:

- Creación y configuración de la base de datos PostgreSQL
- Generación de certificados
- Sincronización de feeds (NVTs, SCAP, CERT)
- Creación del usuario `admin`

⚠️ Este proceso puede tardar varios minutos. Se recomienda no interrumpirlo.

4. Verificar la instalación

Al finalizar `gvm-setup`, valida el estado completo del sistema con:

sudo gvm-check-setup

- ✅ Mensajes en **verde** indican que todo está correctamente instalado.
- ❌ Mensajes en **rojo** indican componentes faltantes o errores (puedes consultarme para solucionarlos).

5. Iniciar los servicios de GVM

Para iniciar el sistema de escaneo y la interfaz web:

sudo gvm-start

Esto:

- Lanza `ospd-openvas`
- Inicia `gsad` (interfaz web en HTTPS)

Deberías ver un mensaje con la URL de acceso:

https://127.0.0.1:9392

6. Acceder a la interfaz web

Desde tu navegador en Kali, abre:

https://localhost:9392

Utiliza el siguiente acceso por defecto (o el que hayas definido):

- Usuario: `admin`
- Contraseña: generada en `gvm-setup` o personalizada

7. Validar el acceso del usuario `admin` vía socket GMP

Si necesitas validar o probar el acceso del usuario `admin` desde consola (sin la interfaz web), puedes hacerlo con el siguiente comando:

```
sudo runuser -u _gvm -- gvm-cli socket --socketpath /run/gvmd/gvmd.sock --xml "$(cat <<EOF

<authenticate>

  <credentials>

    <username>admin</username>

    <password>admin1234</password>

  </credentials>

</authenticate>

EOF

)"
```

Este comando:

- Se conecta al socket GMP (`/run/gvmd/gvmd.sock`)
- Autentica al usuario `admin` con la contraseña `admin1234`

Si es exitoso, obtendrás una respuesta como:

```
<authenticate_response status="200" status_text="OK"><role>Admin</role><timezone>UTC</timezone></authenticate_response>
```

> Esto confirma que el usuario y la contraseña son válidos para interactuar con el sistema mediante `gvm-cli`.

8. ¿Olvidaste la contraseña?

Si necesitas forzar una nueva contraseña para `admin`, ejecuta:

sudo runuser -u _gvm -- gvmd --user=admin --new-password=admin1234