Laboratorio 13

Introducción

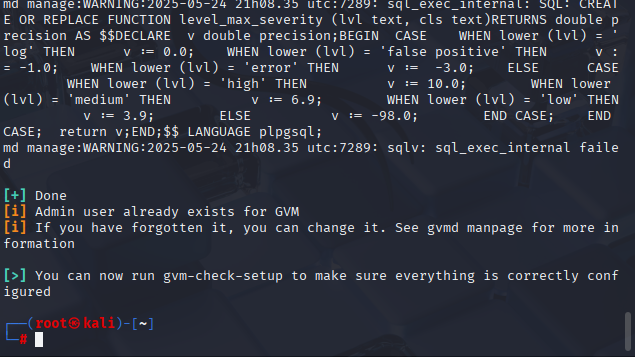
En el ámbito de la ciberseguridad, **un escaneo de vulnerabilidades** es un proceso automatizado que tiene como objetivo identificar debilidades o fallos de seguridad en los sistemas, redes o aplicaciones. Estas vulnerabilidades pueden ser explotadas por atacantes para obtener acceso no autorizado, robar información o causar interrupciones en los servicios. Detectarlas de forma proactiva es fundamental para mitigar riesgos y proteger los activos de una organización.

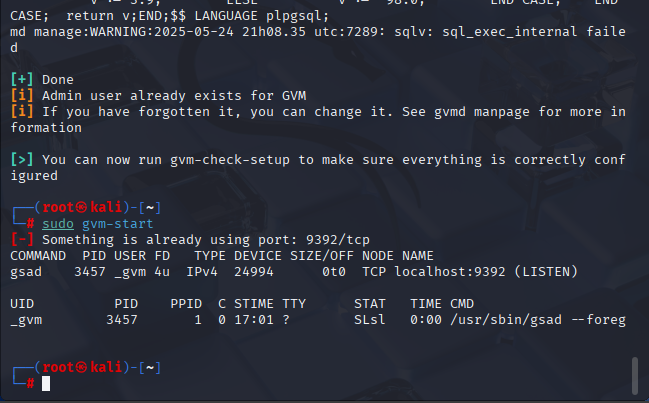
Para llevar a cabo este tipo de análisis, existen herramientas especializadas como **Nessus** o **OpenVAS**. Ambas son escáneres de vulnerabilidades ampliamente utilizados. **Nessus** es una herramienta comercial (con versión gratuita limitada) desarrollada por Tenable, reconocida por su amplia base de datos de vulnerabilidades y facilidad de uso. Por otro lado, **OpenVAS** es una solución de código abierto que forma parte del proyecto Greenbone Vulnerability Management, ideal para entornos que requieren herramientas libres.

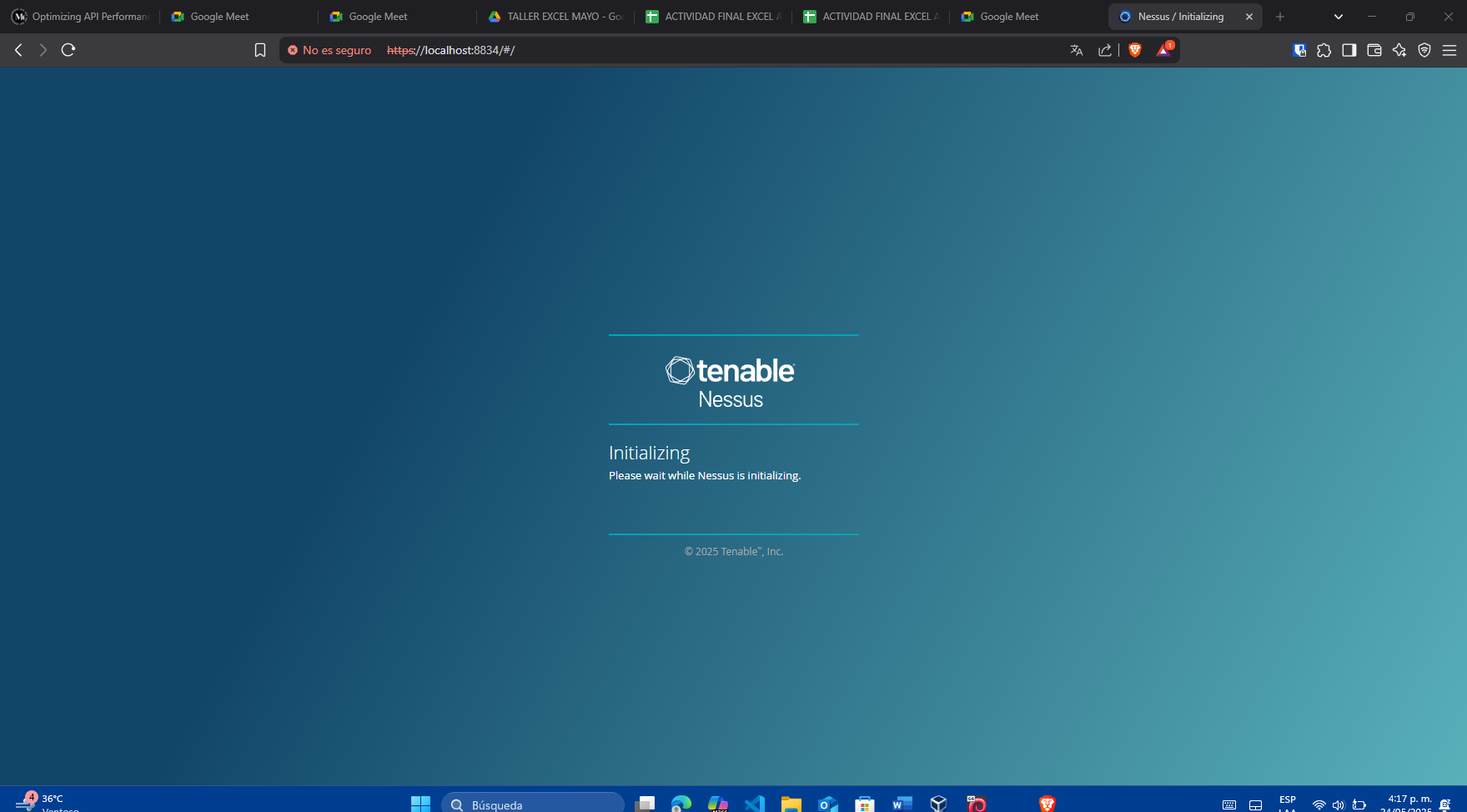
Además, es importante comprender algunos conceptos clave:

* **Vulnerabilidad:** es una debilidad en un sistema que puede ser explotada para comprometer su seguridad.
* **CVSS (Common Vulnerability Scoring System):** es un sistema estandarizado para evaluar la gravedad de las vulnerabilidades. Asigna una puntuación de 0 a 10, donde 10 representa la máxima severidad. Esta puntuación ayuda a priorizar las acciones correctivas basándose en el nivel de riesgo.

Con estas herramientas y conocimientos básicos, es posible mejorar significativamente la postura de seguridad de una organización mediante la identificación y corrección temprana de fallos críticos.







Texto

El contenido generado por IA puede ser incorrecto.

Texto

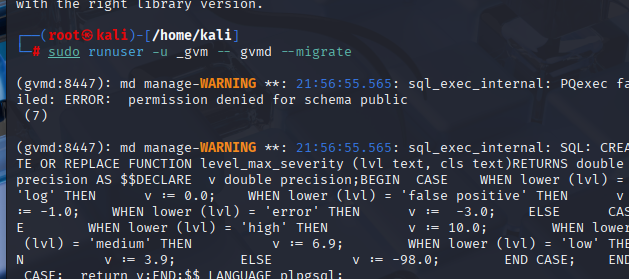
El contenido generado por IA puede ser incorrecto.

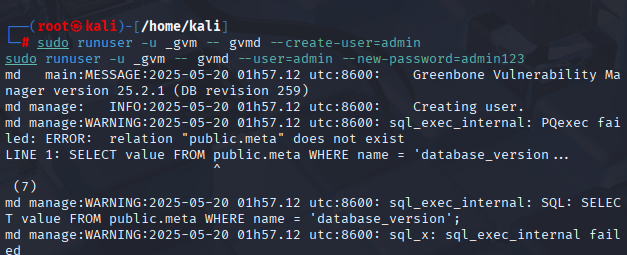
Texto

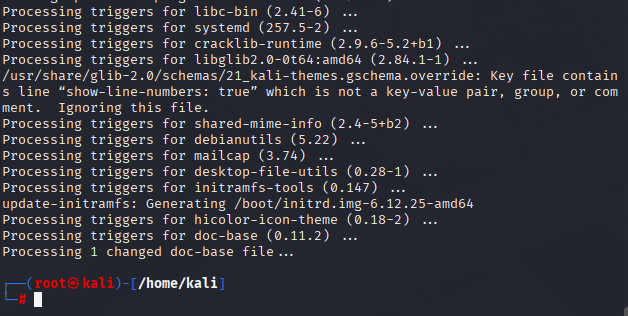
El contenido generado por IA puede ser incorrecto.

Texto

El contenido generado por IA puede ser incorrecto.

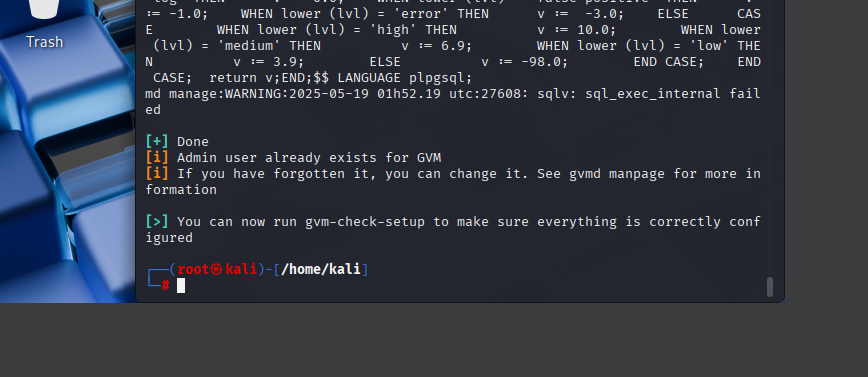


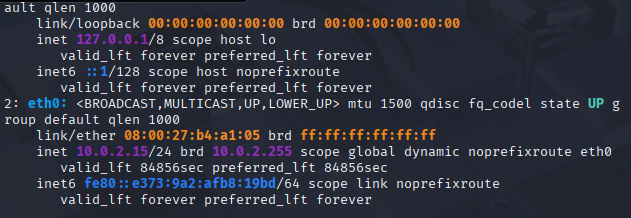


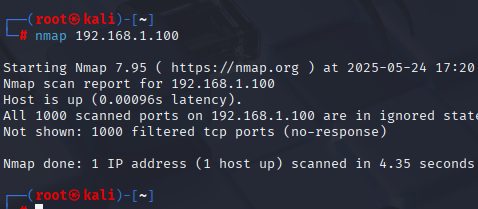


Texto

El contenido generado por IA puede ser incorrecto.







Texto

El contenido generado por IA puede ser incorrecto.

Texto

El contenido generado por IA puede ser incorrecto.