**• Para qué sirve la herramienta y que tipo de prueba no funcional está abarcando**

OpenVAS es un escáner de vulnerabilidades completo que puede detectar una amplia gama de vulnerabilidades en sistemas informáticos y redes. Se utiliza para evaluar la seguridad de un sistema o red, identificando posibles vulnerabilidades que podrían ser explotadas por un atacante.

OpenVAS abarca una variedad de tipos de pruebas no funcionales, incluyendo:

* Seguridad: OpenVAS puede detectar vulnerabilidades de seguridad, como fallas de autenticación, fallas de autorización y fallas de integridad.
* Rendimiento: OpenVAS puede medir el rendimiento de un sistema o red, identificando posibles cuellos de botella que podrían afectar el rendimiento.
* Disponibilidad: OpenVAS puede probar la disponibilidad de un sistema o red, identificando posibles puntos de falla que podrían afectar la disponibilidad.
* Usabilidad: OpenVAS puede evaluar la facilidad de uso de un sistema o red, identificando posibles problemas de usabilidad que podrían afectar la satisfacción del usuario.

En resumen, OpenVAS es una herramienta versátil que se puede utilizar para evaluar una amplia gama de aspectos no funcionales de un sistema o red.

Aquí hay algunos ejemplos específicos de cómo se puede utilizar OpenVAS para realizar pruebas no funcionales:

* Para evaluar la seguridad de un sistema web, OpenVAS se puede utilizar para escanear el sistema en busca de vulnerabilidades de seguridad comunes, como fallas de inyección de código y fallas de Cross-Site Scripting (XSS).
* Para evaluar el rendimiento de una base de datos, OpenVAS se puede utilizar para ejecutar pruebas de carga en la base de datos para identificar posibles cuellos de botella.
* Para evaluar la disponibilidad de un sitio web, OpenVAS se puede utilizar para realizar pruebas de ping y traceroute al sitio web para identificar posibles problemas de conectividad.
* Para evaluar la facilidad de uso de un sistema operativo, OpenVAS se puede utilizar para ejecutar pruebas de usabilidad del sistema operativo para identificar posibles problemas de usabilidad.

**• ¿Para qué se utiliza principalmente en el proceso de desarrollo de software?**

OpenVAS se utiliza principalmente en el proceso de desarrollo de software para evaluar la seguridad de un sistema o red antes de que se implemente. Se puede utilizar para identificar posibles vulnerabilidades que podrían ser explotadas por un atacante.

OpenVAS se puede utilizar en una variedad de etapas del proceso de desarrollo de software, incluyendo:

* Diseño: OpenVAS se puede utilizar para evaluar la seguridad de un diseño de sistema o red, identificando posibles vulnerabilidades que podrían introducirse en el sistema durante el desarrollo.
* Implementación: OpenVAS se puede utilizar para escanear el sistema o red implementado para identificar posibles vulnerabilidades que podrían haberse introducido durante el proceso de implementación.
* Pruebas: OpenVAS se puede utilizar para realizar pruebas de penetración en el sistema o red para identificar posibles vulnerabilidades que podrían ser explotadas por un atacante.

OpenVAS es una herramienta valiosa para ayudar a los desarrolladores de software a crear sistemas y redes seguros. Al utilizar OpenVAS, los desarrolladores pueden identificar y corregir posibles vulnerabilidades antes de que se implementen, lo que ayuda a proteger los sistemas y redes de los ataques.

Aquí hay algunos ejemplos específicos de cómo se puede utilizar OpenVAS en el proceso de desarrollo de software:

* Un desarrollador de software puede utilizar OpenVAS para escanear un diseño de sistema web para identificar posibles vulnerabilidades de seguridad, como fallas de inyección de código y fallas de Cross-Site Scripting (XSS).
* Un equipo de pruebas puede utilizar OpenVAS para realizar pruebas de penetración en un sistema operativo para identificar posibles vulnerabilidades que podrían ser explotadas por un atacante.
* Un equipo de seguridad puede utilizar OpenVAS para escanear una red para identificar posibles vulnerabilidades que podrían ser explotadas por un atacante.

En resumen, OpenVAS es una herramienta versátil que se puede utilizar en una variedad de etapas del proceso de desarrollo de software para ayudar a los desarrolladores a crear sistemas y redes seguros.

Específicamente, OpenVAS se utiliza para:

* Identificar vulnerabilidades de seguridad en sistemas y redes.
* Evaluar la seguridad de un sistema o red antes de que se implemente.
* Ayuda a los desarrolladores de software a crear sistemas y redes seguros.

OpenVAS es una herramienta valiosa que puede ayudar a los desarrolladores de software a crear sistemas y redes más seguros.