Escáner de vulnerabilidades[Nessus Essentials](https://www.tenable.com/products/nessus/nessus-essentials) **permite escanear la red doméstica personal con la misma alta velocidad, evaluaciones a profundidad o buscar vulnerabilidades de forma automatizada.**

**Esta enfocado a analizar las redes informáticas** (Todo lo que tenga sistema operativo, como sistemas embebidos, dispositivos considerados como parte del IoT, etc.)

## ¿Qué escanea?

* Puertos abiertos
* Versiones de los servicios
* Detecta e indica las vulnerabilidades de cada dispositivo y puertos

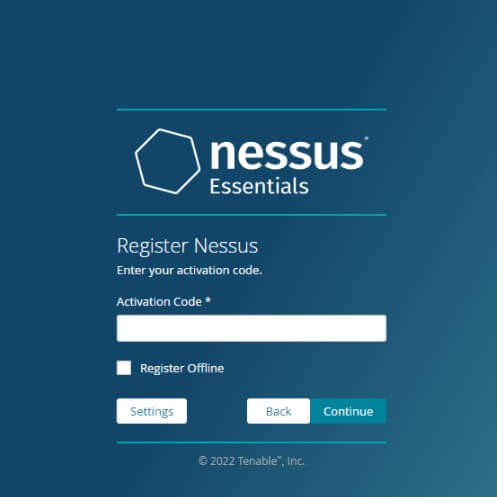
**Nessus no esta especializado en aplicaciones web** 🚩

## Importante 💡

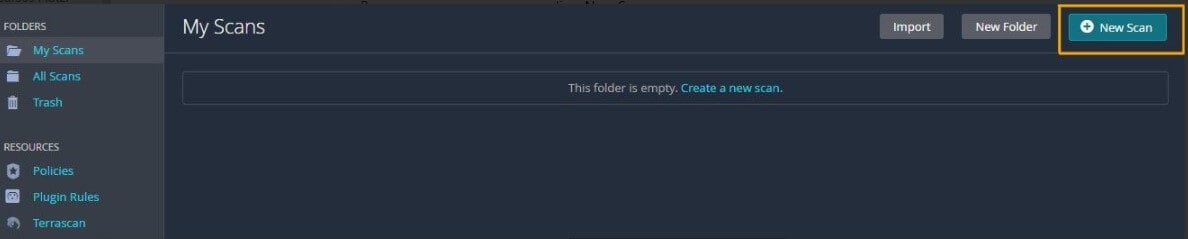
Se debe crear una cuenta **para obtener la clave para la versión essentials.**

Al dar clic a empezar, se va a redireccionar a la sección para descargar Nessus.

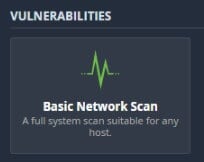
* Buscar versión para el SO ha utilizar

Una vez ejecutado y aceptado los términos, activar el código (Revisar la bandeja de correos) 

Después se creara una cuenta de usuario o iniciar sesión si ya se ha creado la cuenta.

Para crear un nuevo escaneo, clic a **New Scan** 

## Basic Network Scan



## ¿Qué se identifica?

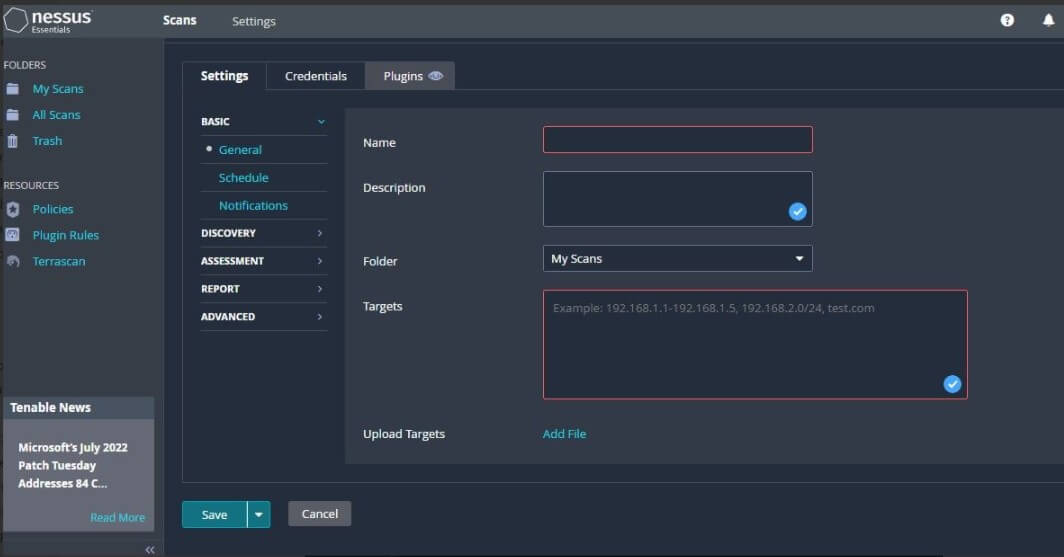
* Los dispositivos de la red
* Puertos abiertos
* Vulnerabilidades (de los puertos abiertos que estén)

**¿Cómo se realiza el scaneo?**

Al dar clic aparecerá la configuración para el escaneo.

**Apartados obligatorios:**

* Nombre
* Targets (Aquí se coloca la IP a escanear)



Una vez configurado, clic a **Save** y se abrirá un nuevo panel de los dispositivos vulnerables.

### Nota 💡

* La versión gratuita esta limitada comparada a la versión empresarial.

Nessus Essentials es una versión gratuita de Nessus, una herramienta ampliamente utilizada para la detección de vulnerabilidades en sistemas informáticos. Está diseñada para proporcionar a los profesionales de la seguridad una herramienta robusta para evaluar la seguridad de sus redes y sistemas, con algunas limitaciones en comparación con las versiones comerciales de Nessus.

### Características de Nessus Essentials

1. **Escaneo de Vulnerabilidades**: Escanea sistemas en busca de una amplia gama de vulnerabilidades, incluyendo configuraciones incorrectas, software desactualizado, y más.
2. **Informes Detallados**: Genera informes detallados sobre las vulnerabilidades encontradas, junto con recomendaciones para la remediación.
3. **Facilidad de Uso**: Interfaz amigable y fácil de usar, apta tanto para principiantes como para usuarios avanzados.
4. **Limitaciones**: Limitado a escanear un máximo de 16 direcciones IP.

### Instalación y Configuración

#### Paso 1: Registro y Descarga

1. Regístrate en la página oficial de Nessus Essentials para obtener una clave de activación gratuita.
2. Descarga el instalador adecuado para tu sistema operativo (Windows, macOS, Linux).

#### Paso 2: Instalación

1. Ejecuta el instalador descargado y sigue las instrucciones en pantalla.
2. Una vez completada la instalación, Nessus se iniciará automáticamente y se abrirá una ventana del navegador para la configuración inicial.

#### Paso 3: Configuración Inicial

1. Acepta los términos de uso.
2. Crea una cuenta de usuario para acceder a la interfaz web de Nessus.
3. Introduce la clave de activación obtenida durante el registro.
4. Nessus descargará los plugins necesarios para los escaneos (esto puede tardar unos minutos).

### Uso de Nessus Essentials

#### Paso 1: Crear un Nuevo Escaneo

1. Inicia sesión en la interfaz web de Nessus.
2. Haz clic en "New Scan" (Nuevo escaneo).
3. Selecciona el tipo de escaneo que deseas realizar (por ejemplo, "Basic Network Scan").
4. Configura los parámetros del escaneo, como el nombre del escaneo, las direcciones IP o los rangos que deseas escanear.

#### Paso 2: Ejecutar el Escaneo

1. Una vez configurado, haz clic en "Save" (Guardar) para guardar el escaneo.
2. Haz clic en el escaneo guardado y luego en "Launch" (Iniciar) para comenzar el escaneo.
3. Nessus ejecutará el escaneo y proporcionará actualizaciones en tiempo real sobre su progreso.

#### Paso 3: Revisar los Resultados

1. Una vez completado el escaneo, haz clic en él para ver los resultados.
2. Revisa las vulnerabilidades encontradas, clasificadas por severidad.
3. Consulta las recomendaciones de remediación para solucionar las vulnerabilidades identificadas.

### Actualización y Mantenimiento

1. Nessus Essentials se actualiza automáticamente para incluir nuevos plugins y reglas de detección de vulnerabilidades.
2. Asegúrate de revisar periódicamente tu instalación de Nessus para asegurarte de que está actualizada y funcionando correctamente.

### Consideraciones Adicionales

* **Limites de IP**: Recuerda que Nessus Essentials está limitado a escanear hasta 16 direcciones IP.
* **Responsabilidad**: Utiliza Nessus de manera ética y legal, escaneando solo redes y sistemas para los que tienes permiso.

Nessus Essentials es una excelente herramienta para los profesionales de la seguridad que desean obtener una visión detallada de las vulnerabilidades en sus sistemas sin incurrir en costos adicionales.