Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Etapa | # 1 Finalizando el Proyecto

Seguridad Informática II

Ingeniería en Desarrollo de Software

TUTOR: Jessica Hernández Romero

ALUMNO: Sarahi Jaqueline Gomez Juárez

FECHA: viernes 30 de enero de 2026

Índice

Introducción:

El presente documento desarrolla de forma detallada una auditoría de vulnerabilidades utilizando la herramienta **Tenable Nessus Essentials**, con el objetivo de identificar riesgos de seguridad en un equipo de cómputo local.

Incluye el proceso completo desde la **instalación y configuración del software**, la **activación de la licencia gratuita**, la **preparación del entorno de análisis**, hasta la **ejecución del escaneo de red** para detectar posibles vulnerabilidades, accesos inseguros y servicios expuestos.

Posteriormente, se documentan las **incidencias encontradas**, mostrando gráficas de severidad, listas de vulnerabilidades, servicios detectados, protocolos activos y detalles técnicos de riesgos como configuraciones inseguras en SMB, OpenSSL, Apache HTTP, SSL y TLS.

El documento también presenta el **reporte visual del análisis**, incluyendo el historial de escaneos, estado de ejecución y resultados consolidados, así como las limitaciones propias de la versión gratuita de Nessus en cuanto a generación de informes y exportación de datos.

Finalmente, se desarrolla un apartado de **Análisis e Identificación de mejoras**, donde se interpretan los resultados obtenidos y se proponen acciones para fortalecer la seguridad del sistema, tales como la actualización de software crítico, la deshabilitación de servicios innecesarios, el refuerzo de configuraciones de red y la implementación de medidas preventivas.

En conjunto, el archivo evidencia la aplicación práctica de técnicas de auditoría de seguridad informática, demostrando cómo detectar vulnerabilidades reales, analizar riesgos y proponer soluciones para prevenir ataques de acceso en sistemas y redes.

Descripción:

El presente proyecto representa un reporte completo de auditoría de seguridad informática enfocado en la detección y prevención de ataques de acceso mediante el uso de la herramienta Nessus Essentials, a lo largo del documento se desarrolla de forma estructurada el proceso de evaluación de vulnerabilidades, iniciando con la instalación y configuración de la herramienta, lo cual permite preparar el entorno de análisis y asegurar que el escaneo se realice correctamente.

Una de las principales características del documento es la sección de **Incidencias encontradas**, donde se documenta el proceso de auditoría y los resultados obtenidos durante el escaneo del equipo local, en este apartado se muestran las evidencias del análisis de seguridad mediante capturas de pantalla que reflejan la ejecución del escaneo, los gráficos de severidad de vulnerabilidades, la identificación del host analizado, así como el listado de servicios activos y configuraciones detectadas. Esta sección permite visualizar de manera clara los posibles riesgos presentes en el sistema, tales como vulnerabilidades en componentes críticos como OpenSSL, Apache HTTP y protocolos de comunicación como SMB, SSL y TLS, evidenciando la exposición del sistema ante posibles ataques.

Posteriormente, el documento incorpora el apartado de **Reporte**, el cual presenta los resultados consolidados del análisis realizado por Nessus Essentials. En esta sección se incluye el historial de escaneos, el estado de ejecución y finalización de la auditoría, así como las vistas generales de los hallazgos detectados, aunque la versión gratuita de la herramienta no permite la generación de informes automatizados, el documento suple esta limitación mediante capturas de pantalla que funcionan como evidencia visual del reporte, permitiendo documentar de forma clara el alcance del análisis y los resultados obtenidos.

Finalmente, se desarrolla el apartado de **Análisis e Identificación de mejoras**, el cual constituye una de las secciones más importantes del documento desde el punto de vista de la seguridad informática. En este segmento se interpretan los resultados obtenidos durante la auditoría, identificando los principales riesgos que afectan al sistema y proponiendo acciones concretas para fortalecer su seguridad. Entre las mejoras sugeridas se destacan la actualización de software vulnerable, la revisión de configuraciones de red, la deshabilitación de servicios innecesarios y la implementación de buenas prácticas de seguridad, con el objetivo de reducir la superficie de ataque y prevenir futuros incidentes de acceso no autorizado.

En conjunto, el documento se caracteriza por su enfoque práctico y técnico, sustentado en evidencias reales de auditoría, así como por su análisis reflexivo orientado a la mejora continua de la seguridad del sistema. La integración de las secciones de incidencias, reporte y análisis de mejoras permite presentar una visión completa del proceso de evaluación de vulnerabilidades, desde la detección de riesgos hasta la propuesta de soluciones, consolidando el trabajo como un ejercicio integral de seguridad informática.

Justificación:

El presente documento tiene como objetivo la realización de una auditoría de vulnerabilidades mediante la herramienta Tenable Nessus Essentials resulta fundamental dentro del ámbito de la seguridad informática, ya que permite identificar de manera preventiva los riesgos que pueden afectar la integridad, confidencialidad y disponibilidad de los sistemas de cómputo y redes, en un contexto donde los ataques cibernéticos son cada vez más frecuentes y sofisticados, la evaluación continua de vulnerabilidades se convierte en una práctica indispensable para proteger la información y los recursos tecnológicos.

Este proyecto se justifica por la necesidad de aplicar técnicas reales de detección y prevención de ataques de acceso, utilizando una herramienta profesional ampliamente reconocida en el área de la ciberseguridad, a través del proceso de instalación, configuración y ejecución del escaneo de vulnerabilidades, se logró simular una auditoría auténtica, permitiendo observar cómo incluso un equipo común puede presentar múltiples exposiciones de seguridad, tales como servicios activos innecesarios, configuraciones visibles desde la red y vulnerabilidades asociadas a componentes críticos como OpenSSL, Apache HTTP, SMB, SSL y TLS.

Asimismo, la documentación detallada de las incidencias encontradas y del reporte visual generado por Nessus Essentials proporciona evidencia clara del análisis realizado, fortaleciendo el aprendizaje práctico y el entendimiento de los riesgos reales que existen en los sistemas informáticos. La inclusión de capturas de pantalla como respaldo del proceso de auditoría permite validar cada etapa del escaneo y demostrar la correcta aplicación de las técnicas de evaluación de seguridad.

Por otra parte, el apartado de Análisis e Identificación de mejoras demuestra la importancia de interpretar los resultados obtenidos y no limitarse únicamente a la detección de vulnerabilidades, sino a proponer acciones concretas de mitigación, como la actualización de software, la deshabilitación de servicios innecesarios, el refuerzo de configuraciones de red y la implementación de medidas preventivas, este enfoque integral de la seguridad informática se orienta no solo a identificar problemas, sino a fortalecer de manera proactiva la postura de seguridad del sistema, promoviendo buenas prácticas de protección de la información.

Finalmente, la auditoría de vulnerabilidades realizada se justifica como una herramienta esencial para la prevención de ataques de acceso, demostrando que la seguridad informática no debe abordarse de forma reactiva, sino preventiva. La identificación temprana de riesgos permite reducir significativamente la posibilidad de incidentes de seguridad, proteger la información y garantizar un funcionamiento más seguro de los sistemas tecnológicos, tanto en entornos profesionales como en el uso cotidiano de los equipos de cómputo.

Desarrollo:

Etapa 1 - Detección y Prevención de Ataques de Acceso

Contextualización:

Se pretende utilizar algunas técnicas de protección ante ataques de explotación y obtención de acceso a sistemas realizando auditorías a la red mediante herramientas tecnológicas ya sean especializadas o que presenten esta funcionalidad de auditoría, en este sentido, se requiere analizar los factores que enfatizan la importancia de la seguridad y que se describen a continuación:

- Prevenir los ataques de acceso.
- Prevenir accesos a las redes
- Monitoreo completo de la red.

Actividad: Instalar y utilizar un software que permita detectar/prevenir ataques de acceso del sistema y la red.

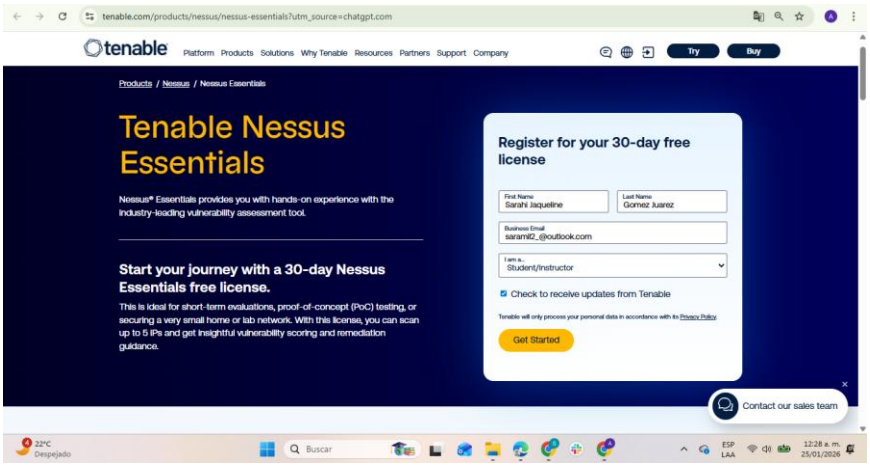
Auditoría de vulnerabilidades en la red:

- Instalar y analizar el equipo.
- Analizar un equipo en búsqueda de posibles ataques como son virus, accesos o percances en red.
- Adjuntar el reporte generado desde la herramienta o capturar el resultado del análisis.

Instalación y configuración de la herramienta de auditoría

Figura 1

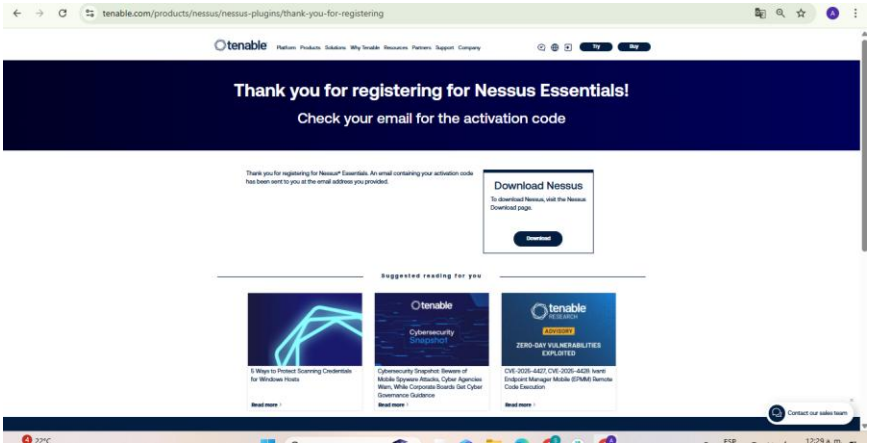
Inicio del asistente de instalación de Tenable Nessus



Nota: Se muestra el asistente inicial que da la bienvenida al usuario para comenzar la instalación del software Nessus.

Figura 2

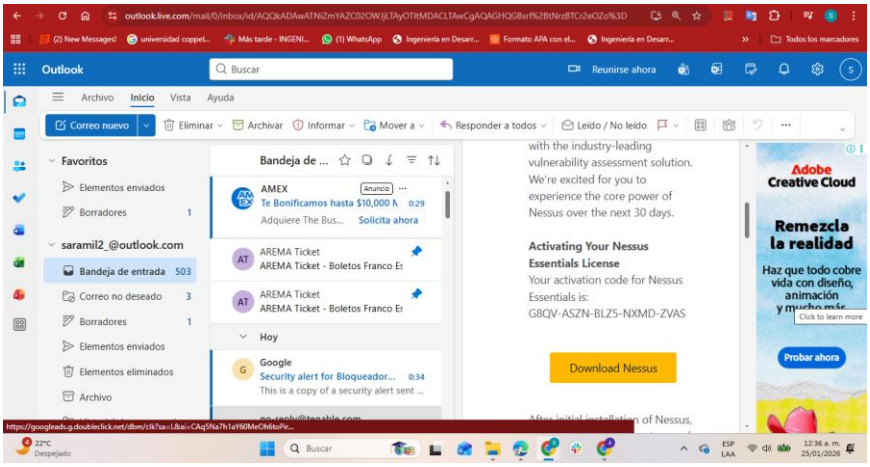
Pantalla de registro para licencia gratuita de Nessus Essentials



Nota: Formulario donde se ingresan los datos personales para obtener la licencia gratuita por 30 días.

Figura 3

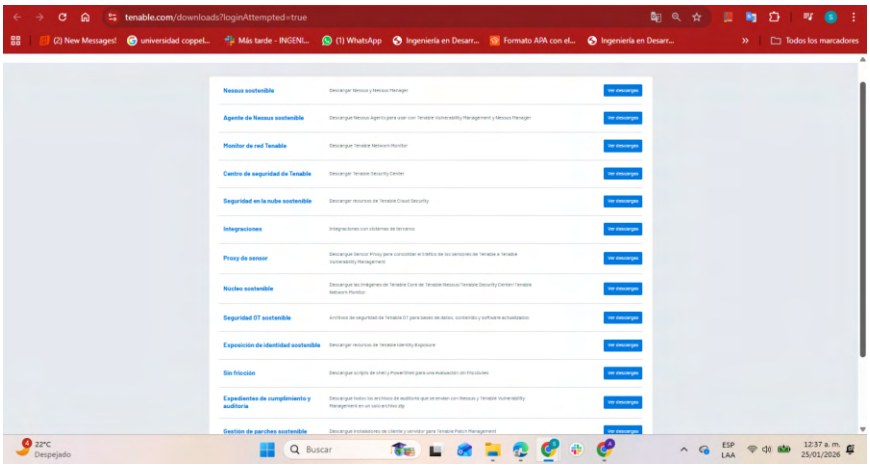
Confirmación de registro exitoso en Tenable



Nota: Pantalla que confirma el registro y solicita revisar el correo para el código de activación.

Figura 4

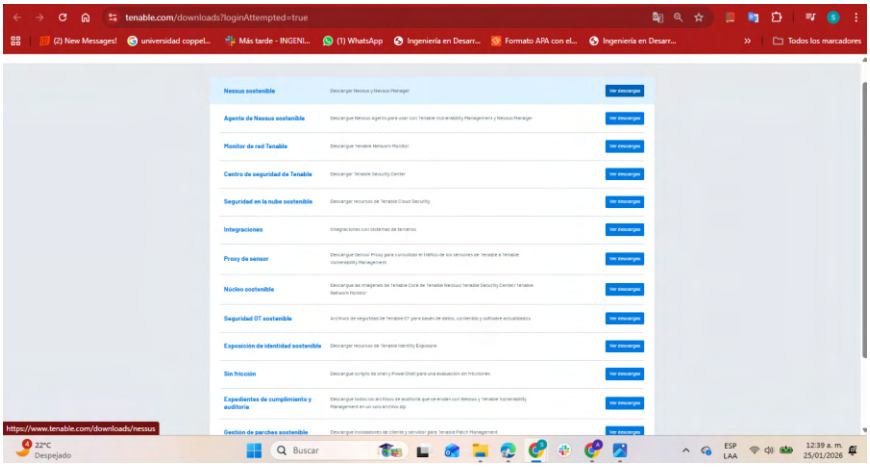
Correo con código de activación de Nessus Essentials



Nota: Correo electrónico recibido con el código de activación de Nessus Essentials, al dar clic nos llevó directamente a la página de descargas de productos Tenable

Figura 5

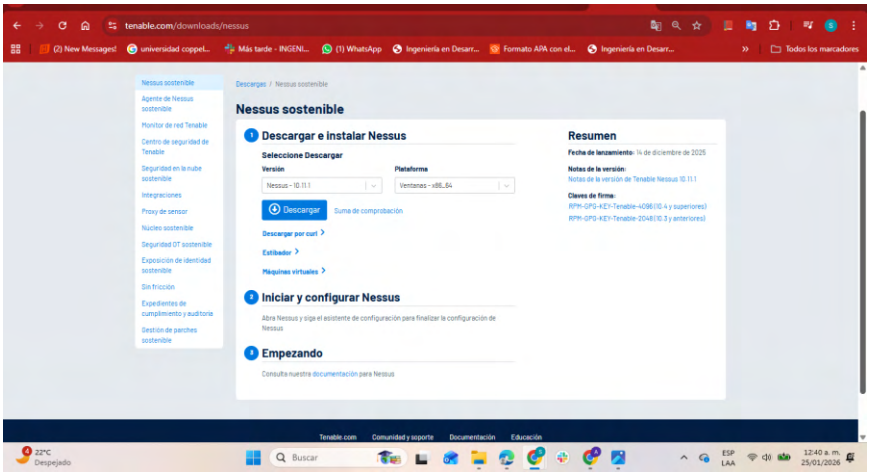
Página de descargas de productos Tenable



Nota: Listado de productos disponibles para descarga en el portal de Tenable.

Figura 6

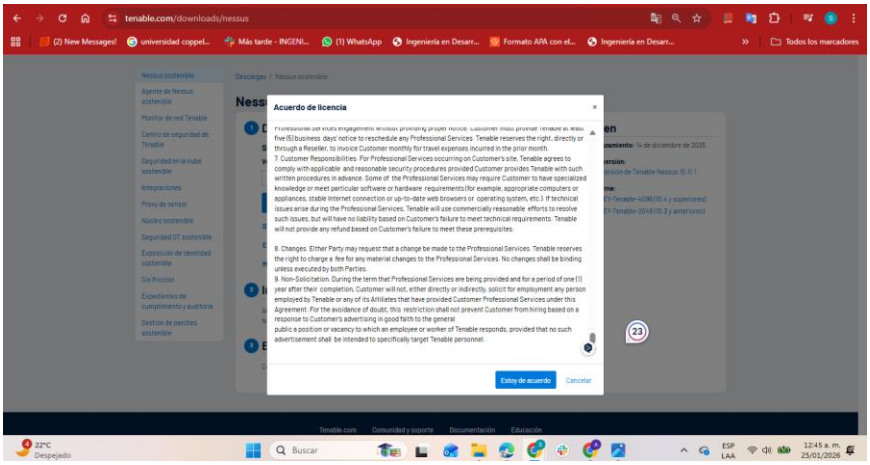
Selección de versión y plataforma para descargar Nessus



Nota: Pantalla donde se selecciona la versión y sistema operativo para instalar Nessus.

Figura 7

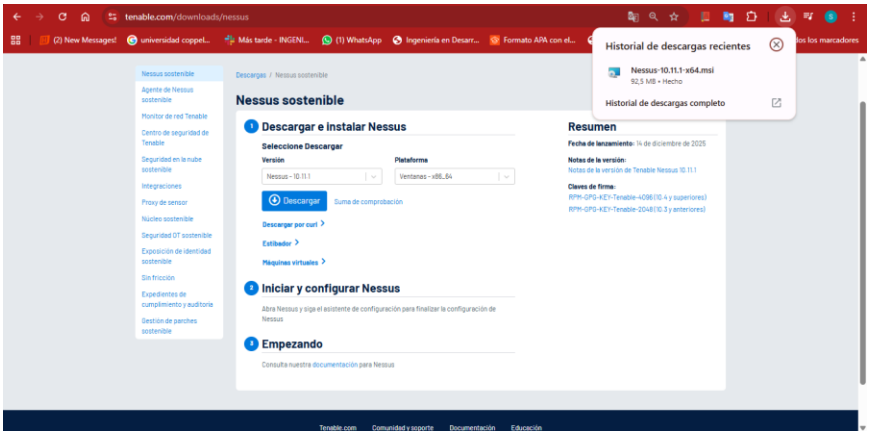
Aceptación del acuerdo de licencia de Nessus



Nota: Ventana del acuerdo de licencia donde se aceptan los términos para continuar la instalación.

Figura 8

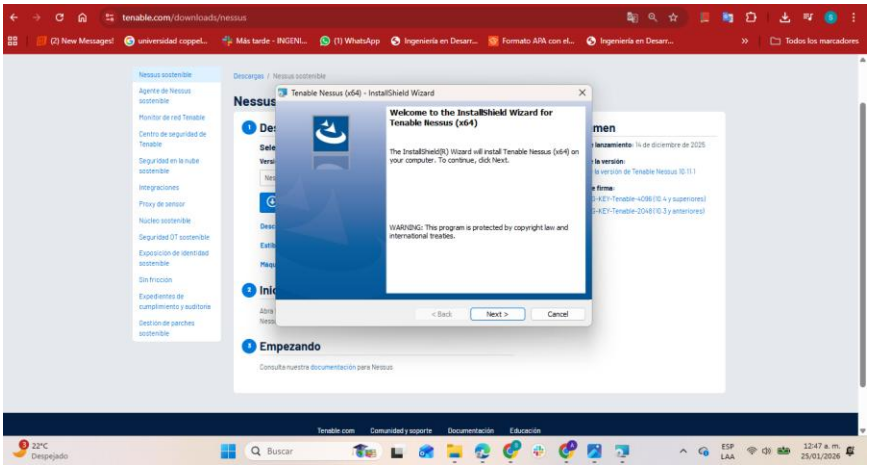
Proceso de descarga completado del instalador



Nota: Mensaje que indica que el archivo instalador se descargó correctamente.

Figura 9

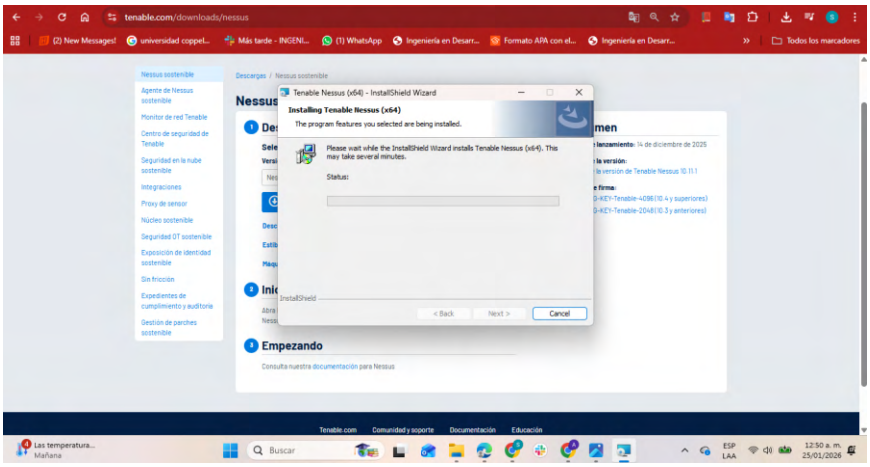
Historial de descargas recientes del navegador



Nota: Panel del navegador mostrando la descarga finalizada del instalador de Nessus.

Figura 10

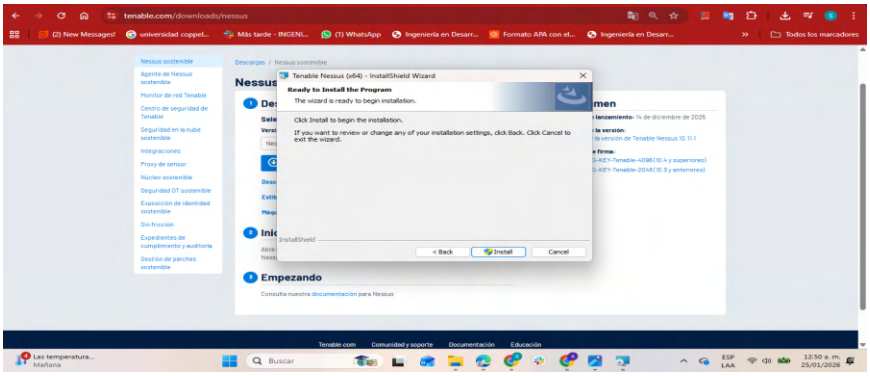
Continuación del asistente de instalación de Nessus



Nota: Pantalla del asistente avanzando en el proceso de instalación.

Figura 11

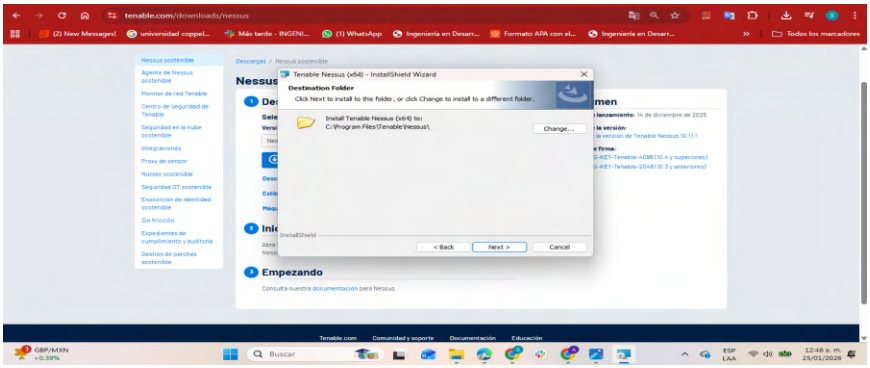
Opciones de despliegue de Nessus



Nota: Se observan las opciones disponibles para registrar o vincular Nessus.

Figura 12

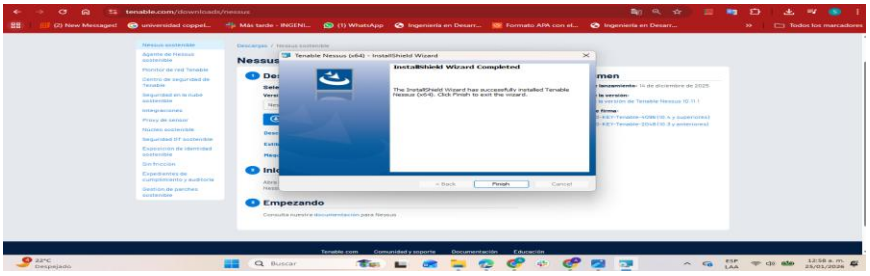
Carpeta de instalación seleccionada



Nota: Indica la ruta donde se instalará el software Nessus.

Figura 13

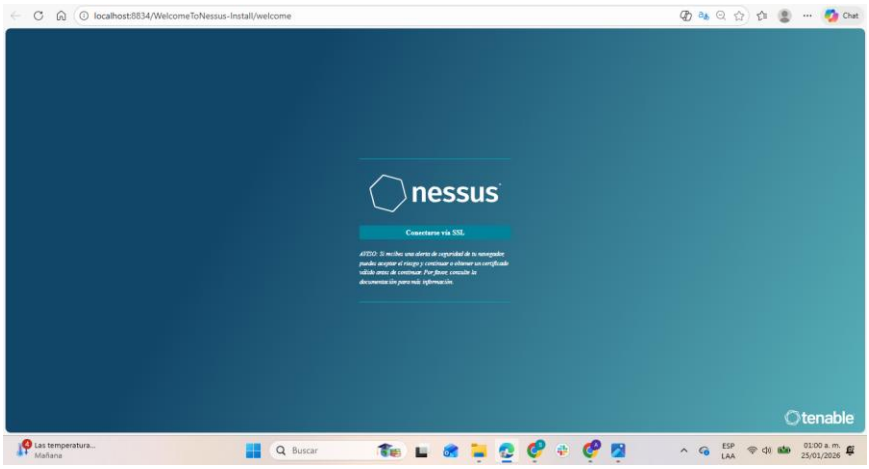
Confirmación para iniciar instalación



Nota: Confirma que el sistema está listo para comenzar la instalación.

Figura 14

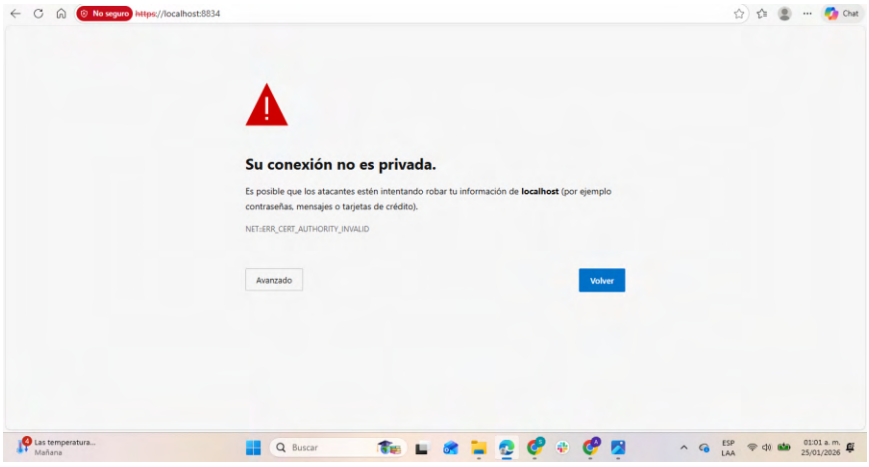
Pantalla inicial de conexión SSL en Nessus



Nota: Se muestra la pantalla inicial posterior a la instalación, donde se seleccionó el botón “Conectarse vía SSL” para acceder a la interfaz web de Nessus mientras la instalación, en la que hay una conexión cifrada.

Figura 15

Advertencia de seguridad del navegador por certificado no válido

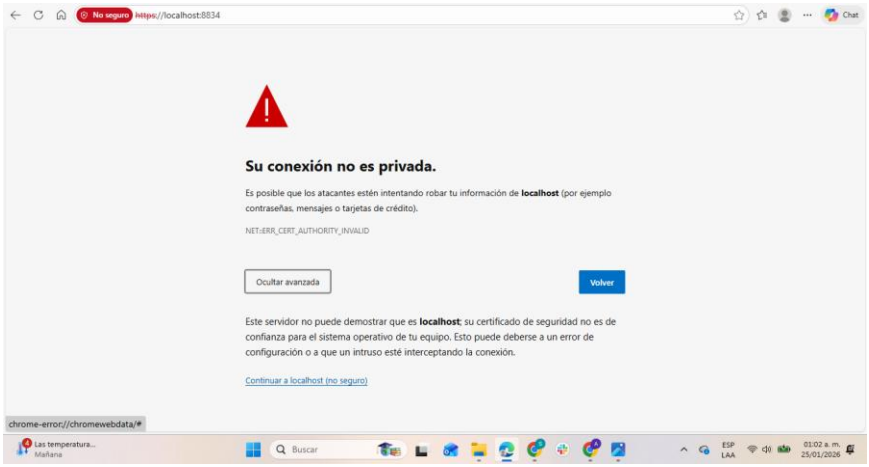


Nota: El navegador bloqueó el acceso a https://localhost:8834 por un certificado no

confiable (NET::ERR_CERT_AUTHORITY_INVALID); para continuar, se hizo clic en el botón “Avanzado”.

Figura 16

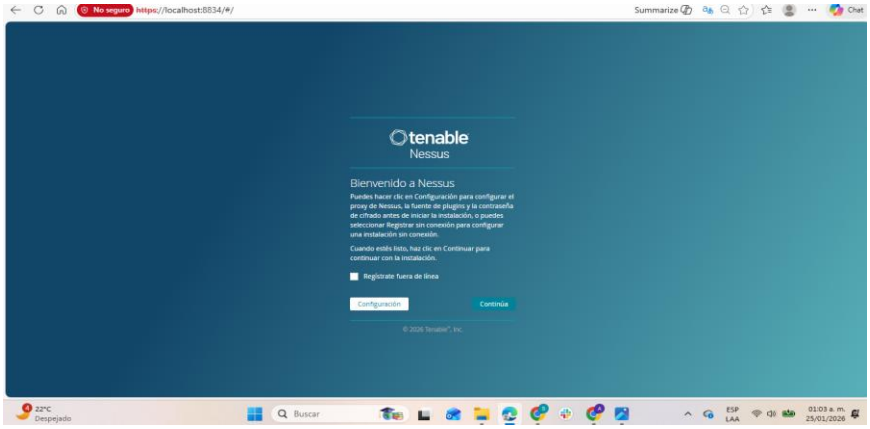
Opción para continuar a localhost sin seguridad



Nota: Tras abrir la sección avanzada, se seleccionó el enlace en azul “Continuar a localhost (no seguro)” para permitir el acceso local a la consola de Nessus.

Figura 17

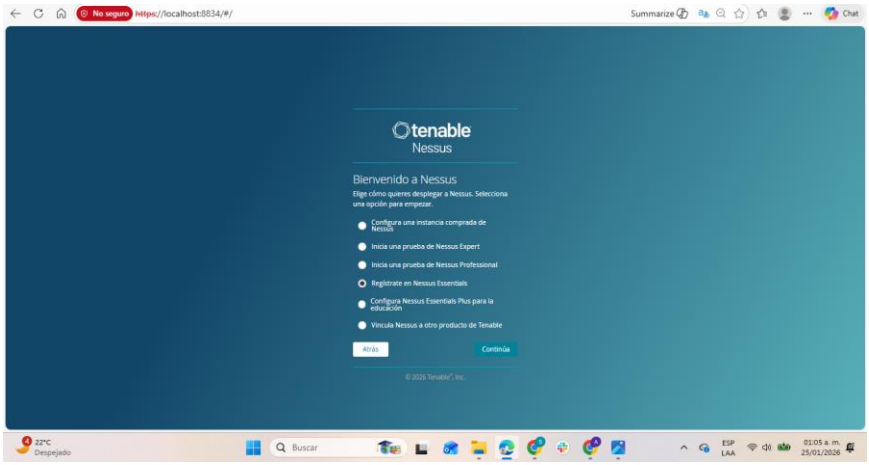
Pantalla de bienvenida de Nessus y selección de “Continúa”



Nota: Se observa la pantalla “Bienvenido a Nessus”; se seleccionó el botón “Continúa” para iniciar el proceso de registro y configuración.

Figura 18

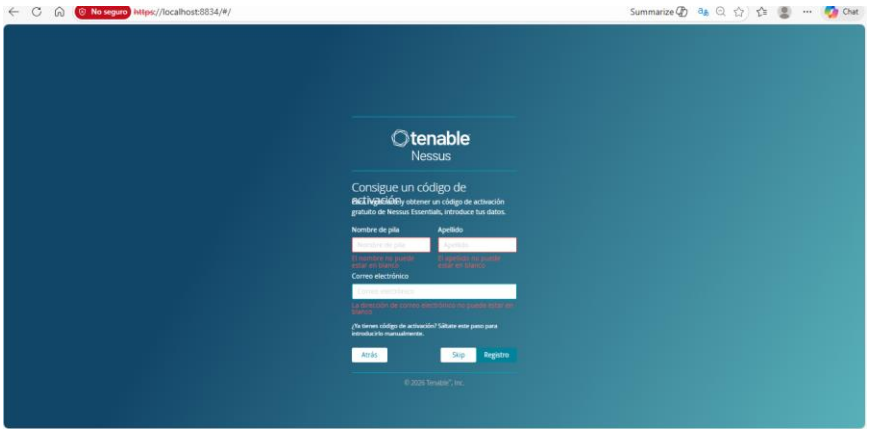
Selección del tipo de despliegue: Registro en Nessus Essentials



Nota: En el menú de opciones se eligió “Regístrate en Nessus Essentials” (opción marcada) y se continuó para activar la licencia gratuita.

Figura 19

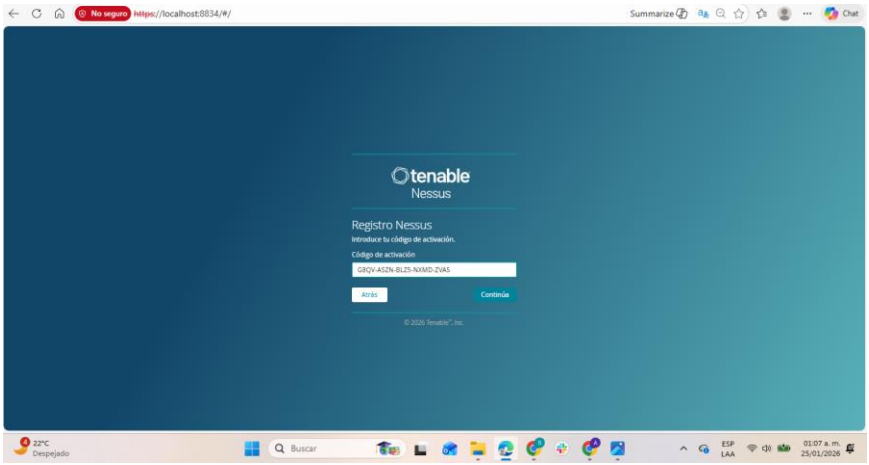
Formulario de registro/activación omitido mediante “Skip”



Nota: Se muestra el formulario para obtener el código de activación; se seleccionó “Skip” porque los datos ya se habían registrado previamente y el código de activación ya había llegado por correo.

Figura 20

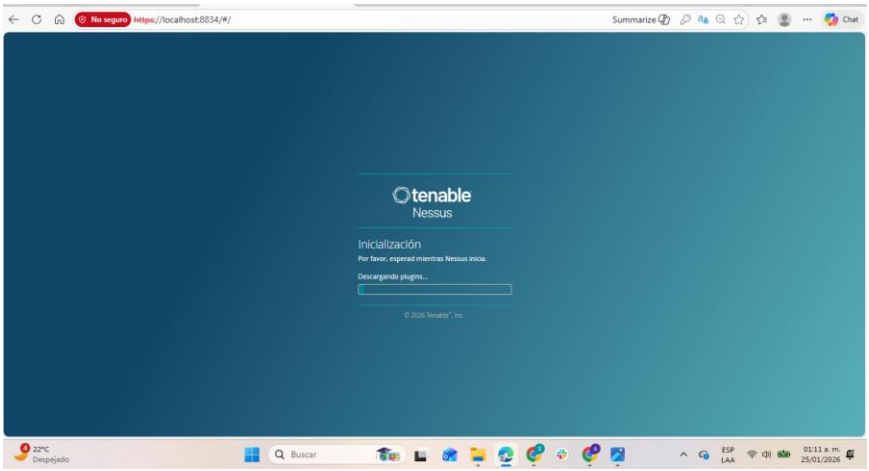
Pantalla de registro de Nessus con código de activación ingresado



Nota: En esta figura se observa pantalla de registro de nessus con código de activación ingresado, mostrando el avance correcto del proceso de instalación y configuración de Nessus Essentials.

Figura 21

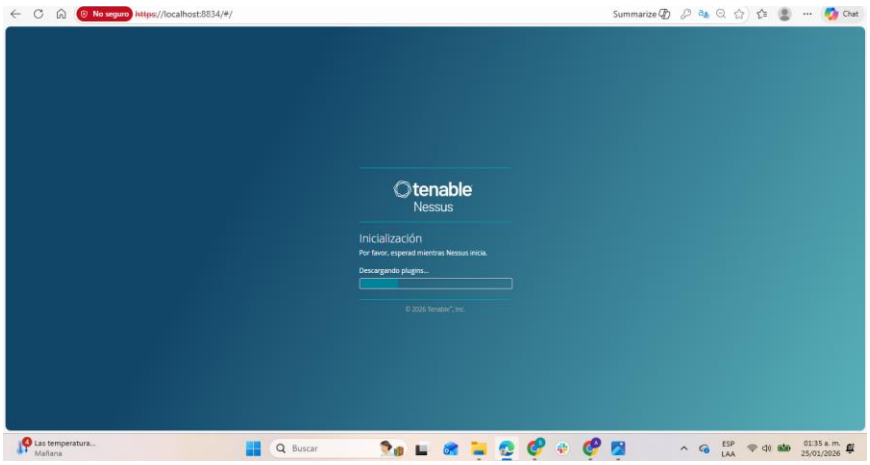
Creación de cuenta de usuario administrador en Nessus



Nota: En esta figura se observa la creación de cuenta de usuario administrador en Nessus, mostrando el avance correcto del proceso de instalación y configuración de Nessus Essentials.

Figura 22

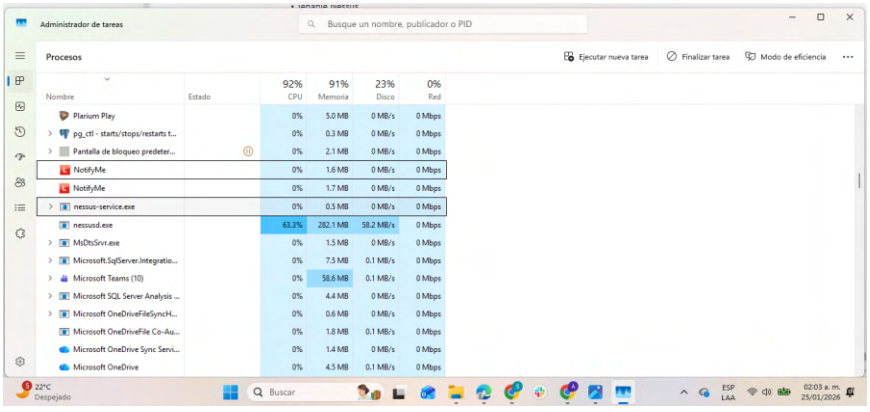
Proceso de inicialización y descarga de plugins



Nota: En esta figura se observa el proceso de inicialización y descarga de plugins, mostrando el avance correcto del proceso de instalación y configuración de Nessus Essentials.

Figura 23

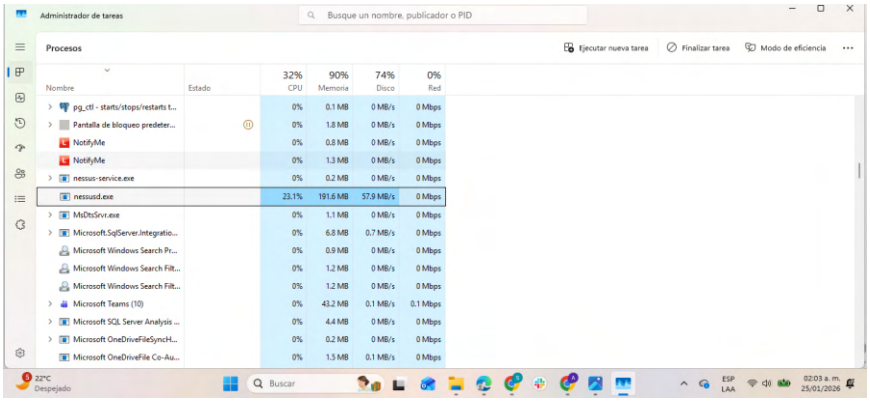
Barra de progreso de descarga de plugins



Nota: En esta figura se observa barra de progreso de descarga de plugins, mostrando el avance correcto del proceso de instalación y configuración de Nessus Essentials.

Figura 24

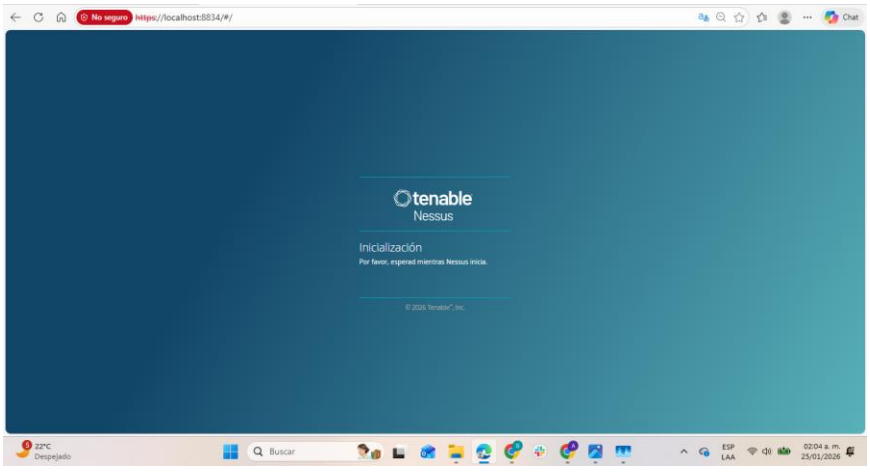
Administrador de tareas mostrando proceso nessusd.exe en ejecución



Nota: En esta figura se observa el administrador de tareas mostrando el proceso nessusd.exe en ejecución, con el avance correcto del proceso de instalación y configuración de Nessus Essentials.

Figura 25

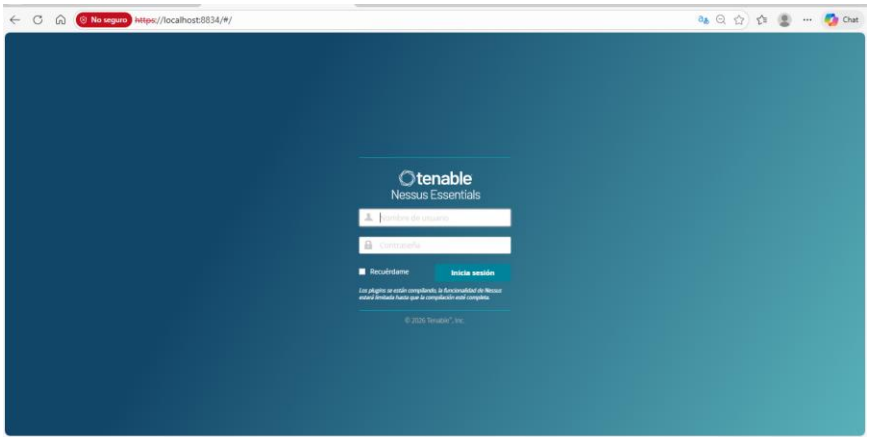
Continuación del proceso de compilación de plugins:



Nota: En esta figura se observa la continuación del proceso de compilación de plugins, mostrando el avance correcto del proceso de instalación y configuración de Nessus Essentials.

Figura 26

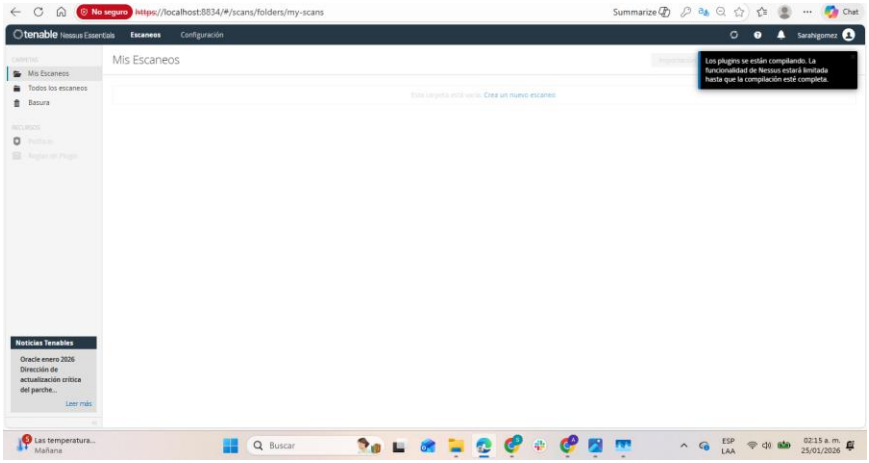
Pantalla de inicio de sesión de Nessus Essentials



Nota: En esta figura se observa la pantalla de inicio de sesión de Nessus Essentials, mostrando el avance correcto del proceso de instalación y configuración de Nessus Essentials.

Figura 27

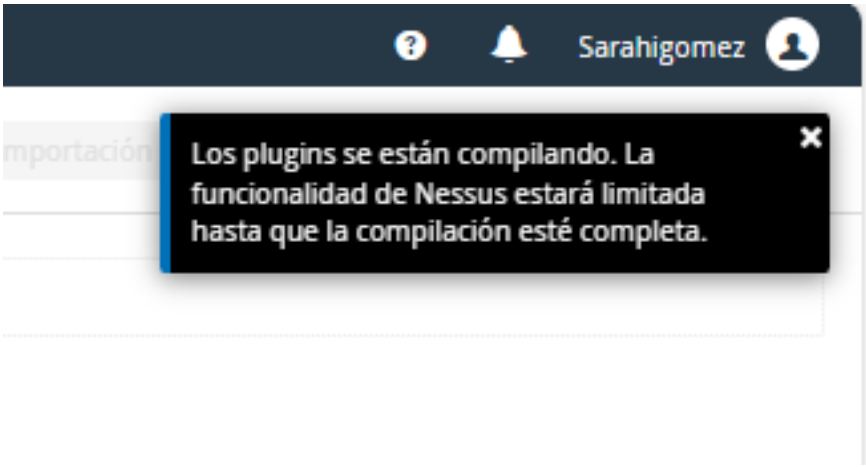
Interfaz principal de Nessus con advertencia de compilación activa



Nota: En esta figura se observa la interfaz principal de Nessus con advertencia de compilación activa, mostrando el avance correcto del proceso de instalación y configuración de Nessus Essentials.

Figura 28

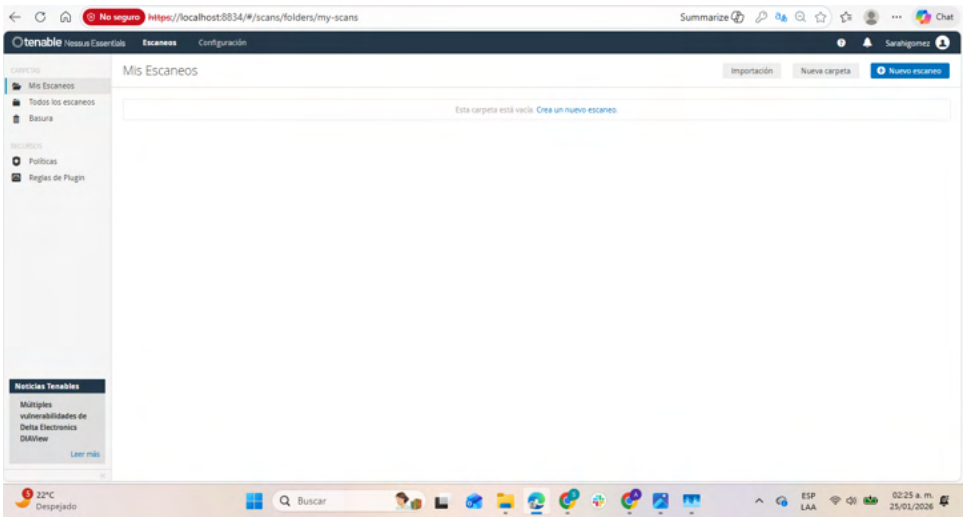
Vista de mis escaneos en Nessus Essentials



Nota: En esta figura se observa la vista de mis escaneos en Nessus Essentials, mostrando el avance correcto del proceso de instalación y configuración de Nessus Essentials.

Figura 29

Interfaz principal de Nessus Essentials – Sección "Mis Escaneos"



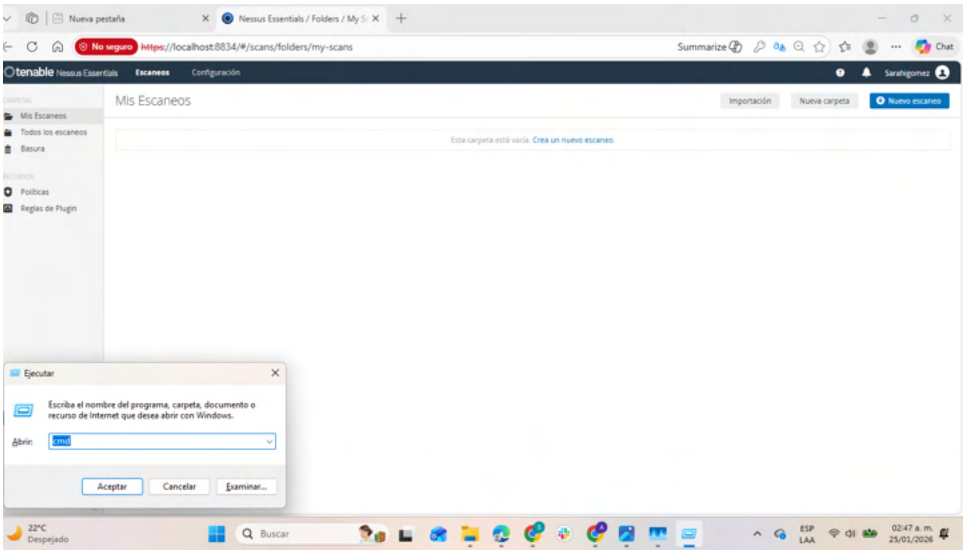
Nota: En esta captura se observa la interfaz principal de Nessus Essentials, específicamente el apartado "Mis Escaneos", el cual permite administrar y visualizar los análisis de vulnerabilidades creados por el usuario, desde una perspectiva de seguridad informática, esta sección es fundamental ya que centraliza la gestión de auditorías, permitiendo organizar

escaneos por carpetas, importar configuraciones previas y lanzar nuevos análisis; la ausencia de escaneos en esta vista inicial indica que aún no se ha ejecutado ningún proceso de evaluación, lo que resalta la importancia de una correcta planeación antes de iniciar pruebas de seguridad, esta interfaz facilita el control del ciclo de vida de auditorías, ayudando a mantener trazabilidad de vulnerabilidades detectadas y evaluaciones históricas.

Se recomienda implementar una política periódica de escaneos para asegurar un monitoreo continuo de la infraestructura.

Figura 30

Uso del símbolo del sistema (CMD) para obtener la configuración IP



Nota: Aquí se muestra el uso del comando ipconfig en el símbolo del sistema de Windows para identificar la configuración de red del equipo local, desde el enfoque de ciberseguridad, este paso es crucial ya que permite conocer la dirección IP que será el objetivo del escaneo de vulnerabilidades. La obtención de datos como IP, máscara de subred y puerta de enlace predeterminada facilita la correcta delimitación del alcance de una auditoría. Esta información también puede ser explotada por atacantes para mapear una red si no se protege

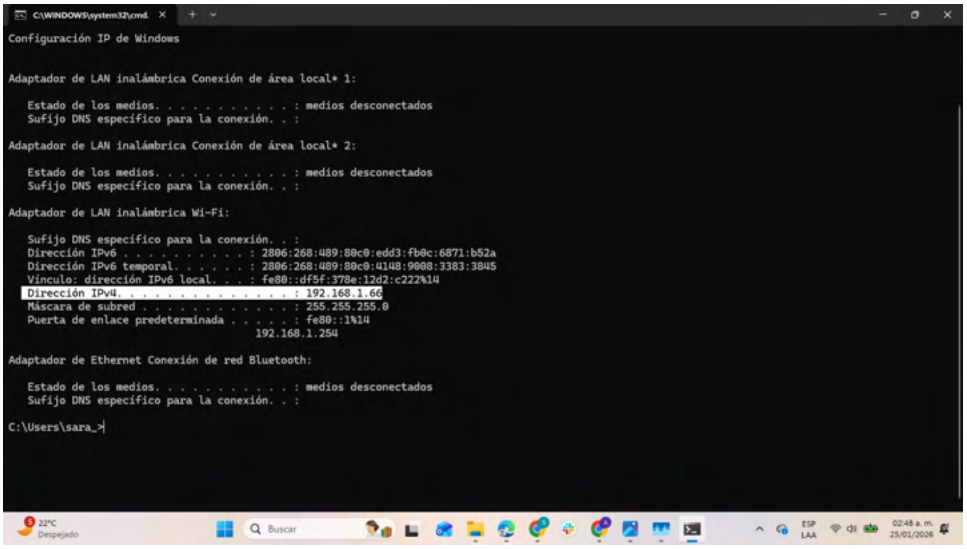
adecuadamente.

Se recomienda implementar y limitar la exposición de información de red y reforzar controles de firewall para evitar el reconocimiento no autorizado.

Incidencias encontradas

Figura 31

Identificación de la dirección IP del equipo a analizar:

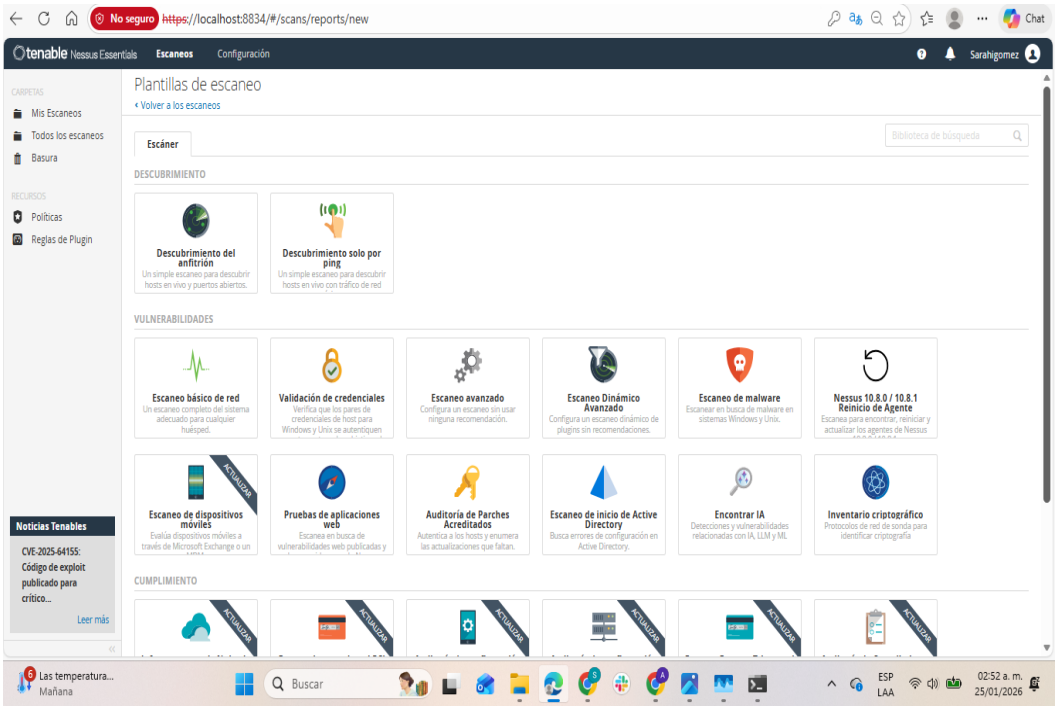


Nota: En esta imagen se resalta la dirección IPv4 del equipo local (192.168.1.66), que será utilizada como objetivo del escaneo en Nessus, esta IP pertenece a una red privada, común en entornos domésticos o corporativos pequeños, desde el punto de vista de seguridad, definir correctamente el host a evaluar es vital para evitar análisis erróneos o fuera de alcance, esta dirección representa el activo que será sometido a revisión de configuraciones, servicios activos y posibles vulnerabilidades.

Se recomienda mantener un inventario actualizado de activos con sus respectivas direcciones IP para una gestión de riesgos más efectiva.

Figura 32

Selección del tipo de escaneo "Escaneo básico de red"

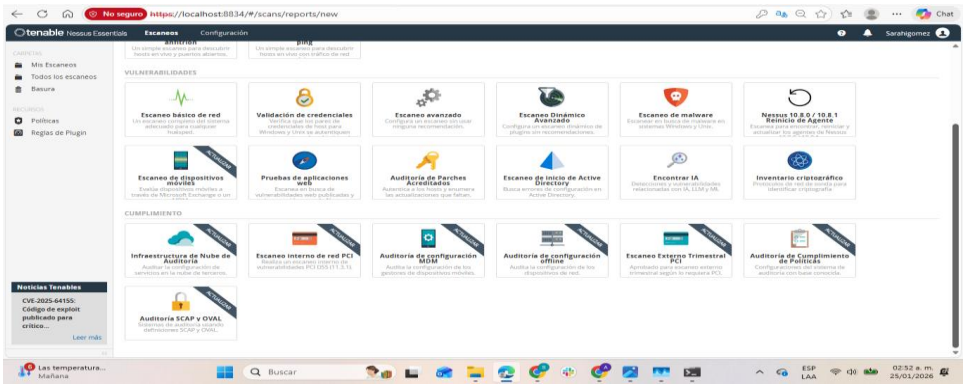


Nota: Aquí se observa la selección de la plantilla "Escaneo básico de red" dentro de Nessus, diseñada para detectar vulnerabilidades comunes en sistemas y dispositivos conectados, este tipo de análisis realiza descubrimiento de puertos abiertos, servicios activos y configuraciones inseguras, desde el enfoque de ciberseguridad, es una herramienta inicial clave para obtener una visión general del estado de seguridad de un equipo o red.

Se recomienda utilizar este escaneo como punto de partida y posteriormente complementar con análisis avanzados o con credenciales.

Figura 33

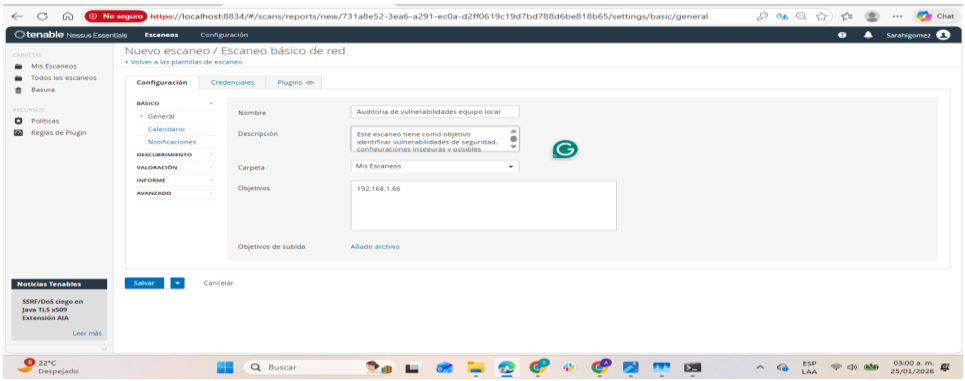
Visualización de otras herramientas de análisis disponibles en Nessus



Nota: Esta captura muestra la variedad de plantillas que ofrece Nessus, incluyendo escaneos de malware, auditorías de parches, análisis de aplicaciones web y evaluaciones de cumplimiento, esto demuestra la capacidad integral de la herramienta para abordar múltiples vectores de riesgo. En términos de ciberseguridad, contar con diversas metodologías de análisis permite una defensa más completa frente a amenazas modernas, por lo que se recomienda implementar distintos tipos de escaneo según el entorno para una cobertura de seguridad más amplia.

Figura 34

Configuración del escaneo básico de red con IP objetivo



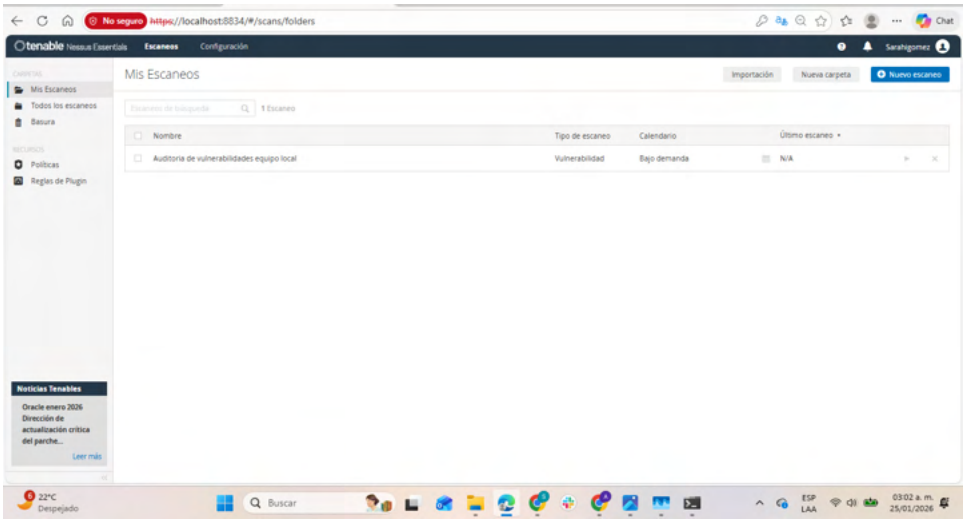
Nota: En esta imagen se observa la configuración del escaneo, donde se asigna un nombre, una descripción y la dirección IP del equipo a analizar, este paso formaliza la auditoría de vulnerabilidades, desde una perspectiva de seguridad informática, una correcta documentación del escaneo ayuda a identificar el propósito de la prueba y facilita auditorías posteriores.

El uso del propio equipo como objetivo permite demostrar cómo Nessus detecta riesgos reales en sistemas comunes.

Por lo que es recomendable incluir siempre descripciones claras para diferenciar auditorías de producción, pruebas o entornos de laboratorio.

Figura 35

Escaneo creado sin haberse ejecutado aún



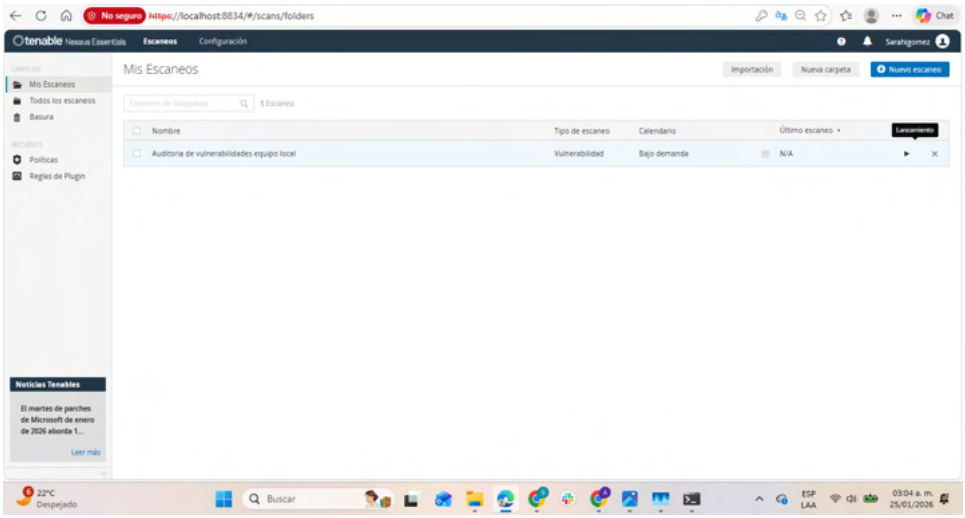
Nota: Aquí se muestra el escaneo ya configurado dentro de la lista de “Mis Escaneos”, pero aún sin iniciar, este estado refleja una fase de preparación antes de ejecutar la evaluación de seguridad. En ciberseguridad, esta etapa es importante para verificar configuraciones y evitar análisis incorrectos que puedan afectar sistemas críticos.

Recomendación: Revisar objetivos y parámetros antes de cada ejecución para asegurar

resultados confiables.

Figura 36

Inicio del escaneo mediante el botón "Play"

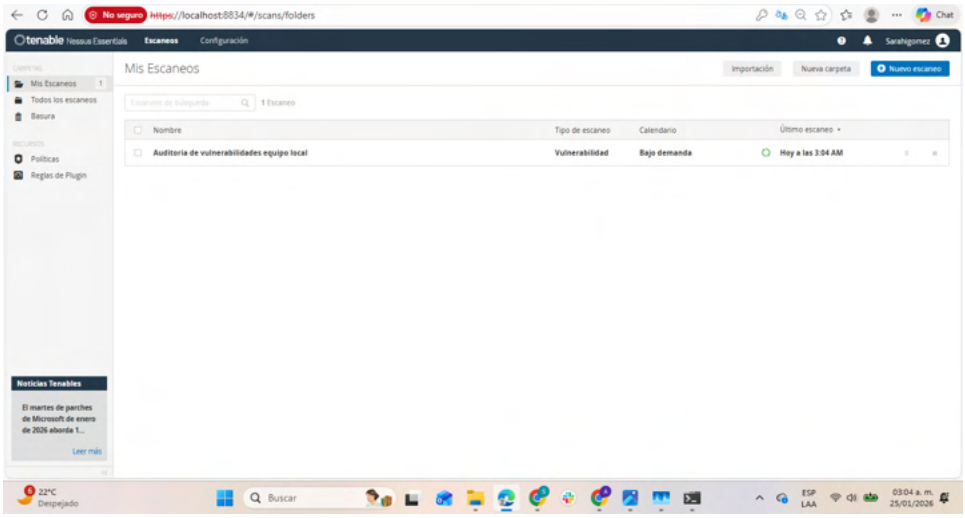


Nota: En esta captura se evidencia la acción de iniciar el escaneo presionando el botón de ejecución, este momento marca el comienzo del análisis activo de vulnerabilidades, donde Nessus comienza a interactuar con el sistema objetivo para identificar puertos abiertos, servicios y posibles fallos de seguridad, este proceso simula técnicas que podrían ser usadas por atacantes para reconocer sistemas vulnerables.

Recomendación: Ejecutar escaneos en horarios controlados para minimizar el impacto en el rendimiento.

Figura 37

Registro de la hora de inicio del escaneo

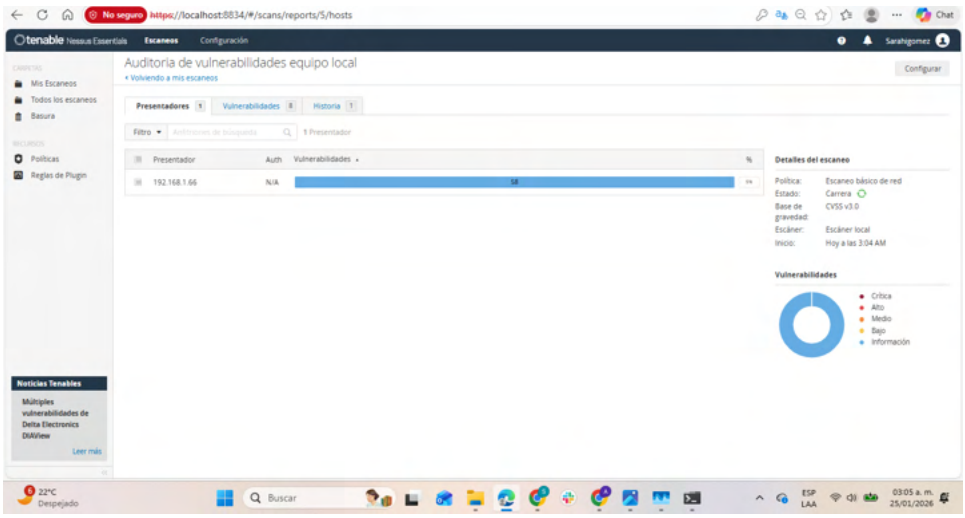


Nota: Aquí se muestra el historial indicando la hora exacta en que comenzó el escaneo (3:04 AM), desde el punto de vista de ciberseguridad, el registro temporal es fundamental para auditorías, análisis forense y seguimiento de cambios en el estado de seguridad, permite comparar resultados entre diferentes momentos y evaluar mejoras o deterioros en la postura de seguridad.

Recomendación: Mantener históricos de escaneos para análisis de tendencias de riesgo.

Figura 38

Resultados iniciales del escaneo con gráfico circular

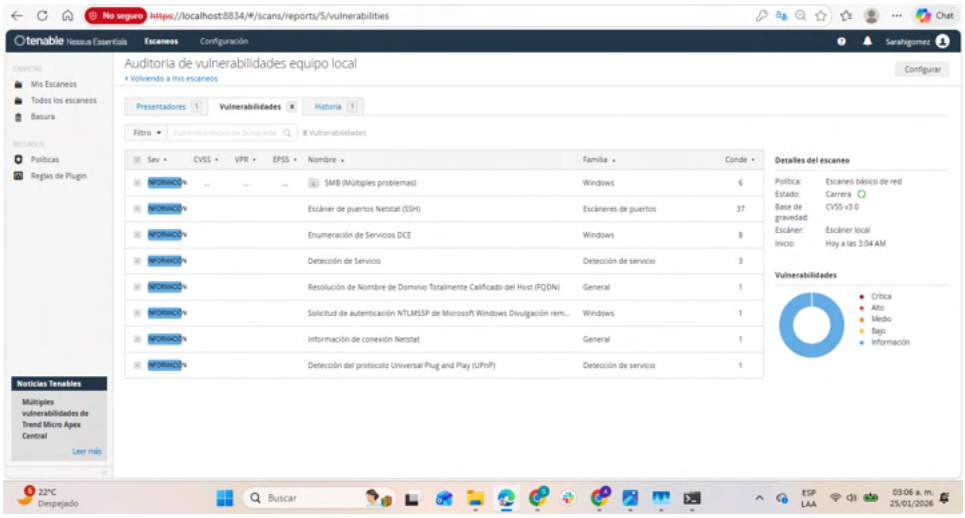


Nota: En esta imagen se observan los primeros resultados del escaneo, incluyendo la sección de presentadores, el conteo de vulnerabilidades detectadas y un gráfico circular que clasifica los hallazgos por nivel de severidad. El predominio del color azul indica vulnerabilidades informativas, mientras que otras secciones representan riesgos mayores que deben atenderse.

Recomendación: Priorizar vulnerabilidades altas y medias sin descuidar las informativas.

Figura 39

Vista general de vulnerabilidades detectadas por Nessus

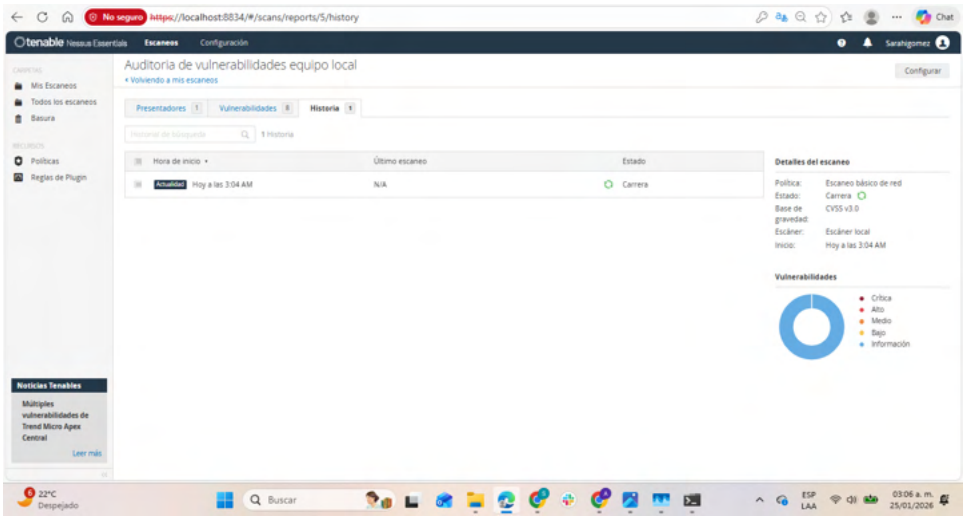


Nota: En esta captura se observa la sección de vulnerabilidades identificadas durante la auditoría del equipo local mediante Nessus Essentials, la herramienta clasifica los hallazgos principalmente como información y algunos de nivel medio, esto indica que, aunque no se detectaron amenazas críticas inmediatas, sí existen configuraciones y servicios expuestos que podrían representar riesgos si no se gestionan correctamente, desde la perspectiva de seguridad informática, este tipo de resultados es común en equipos domésticos o de prueba, donde varios servicios permanecen activos por defecto.

El gráfico circular muestra que la mayoría de los hallazgos corresponden a información, lo cual sugiere que Nessus ha identificado servicios abiertos, protocolos activos y configuraciones visibles desde la red, lo que aumenta la superficie de ataque del sistema.

Figura 40

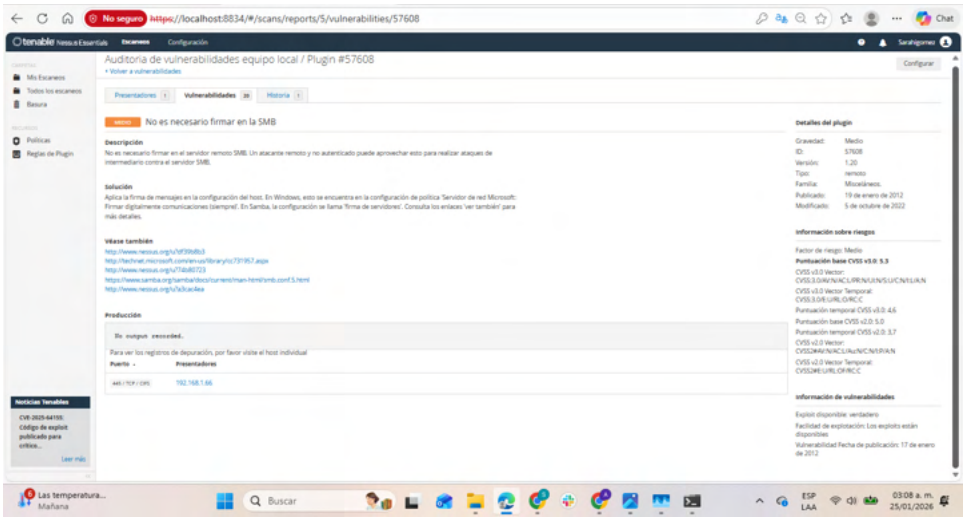
Historial del escaneo de vulnerabilidades



Nota: Aquí se presenta el historial del escaneo ejecutado, mostrando la hora de inicio (3:04 AM) y su estado en proceso o carrera, este apartado es fundamental en auditorías de seguridad, ya que permite dar seguimiento a los análisis realizados, verificar cuándo se ejecutaron y confirmar si concluyeron correctamente, desde un enfoque de ciberseguridad, mantener registros de auditoría es una buena práctica para detectar patrones de vulnerabilidades en el tiempo y evaluar si las medidas de mitigación aplicadas reducen los riesgos en futuros escaneos.

Figura 41

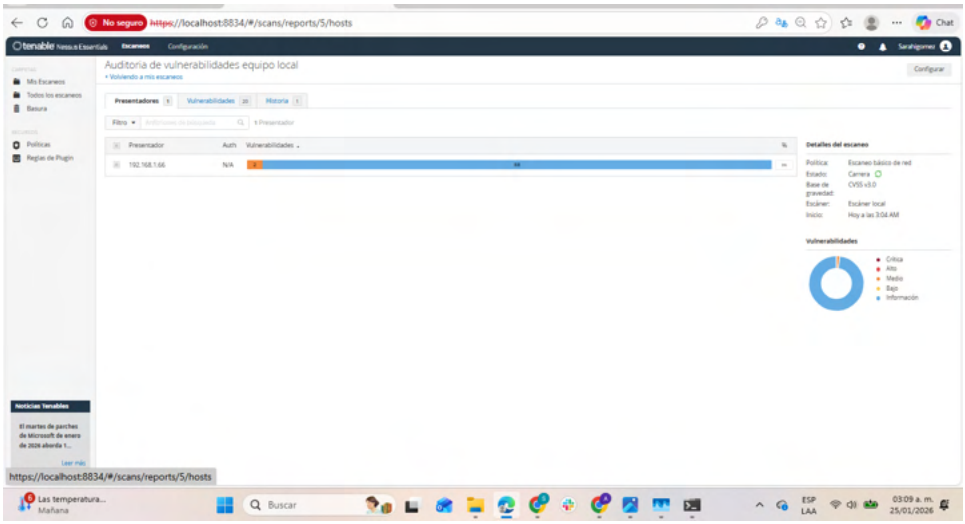
Detalle de una vulnerabilidad específica detectada (SMB sin firma)



Nota: En esta imagen se observa una vulnerabilidad de nivel medio relacionada con el protocolo SMB, indicando que no es necesario firmar las comunicaciones. Esto representa un riesgo importante, ya que permite que atacantes no autenticados puedan interceptar o manipular el tráfico de red, facilitando ataques de tipo intermediario (Man-in-the-Middle). En seguridad informática, SMB sin firma digital es una debilidad conocida que puede ser explotada para robar información o ejecutar comandos de forma remota. La recomendación principal es habilitar la firma de mensajes SMB para asegurar la integridad y autenticidad de las comunicaciones.

Figura 42

Resumen por host analizado (192.168.1.66)

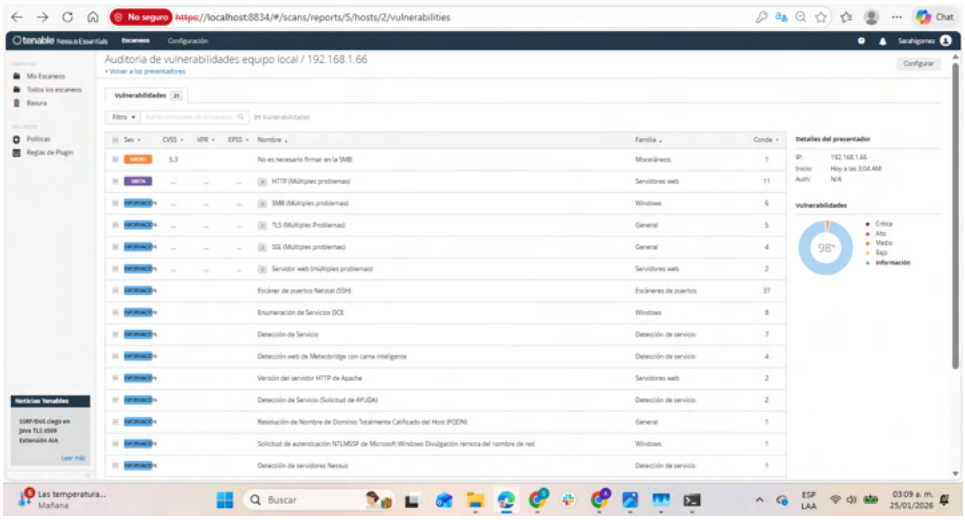


Nota: Esta captura muestra el equipo local identificado por su dirección IP, junto con una barra que representa la cantidad total de vulnerabilidades detectadas, se observa que la mayoría corresponde a hallazgos informativos, mientras que una pequeña porción se clasifica como media.

El gráfico circular refuerza visualmente que el riesgo crítico es bajo, pero no inexistente. En términos de seguridad, esto indica que el sistema no presenta amenazas graves inmediatas, pero sí múltiples servicios expuestos que podrían convertirse en vulnerabilidades reales si un atacante los explota con técnicas más avanzadas.

Figura 43

Lista detallada de vulnerabilidades por categoría:

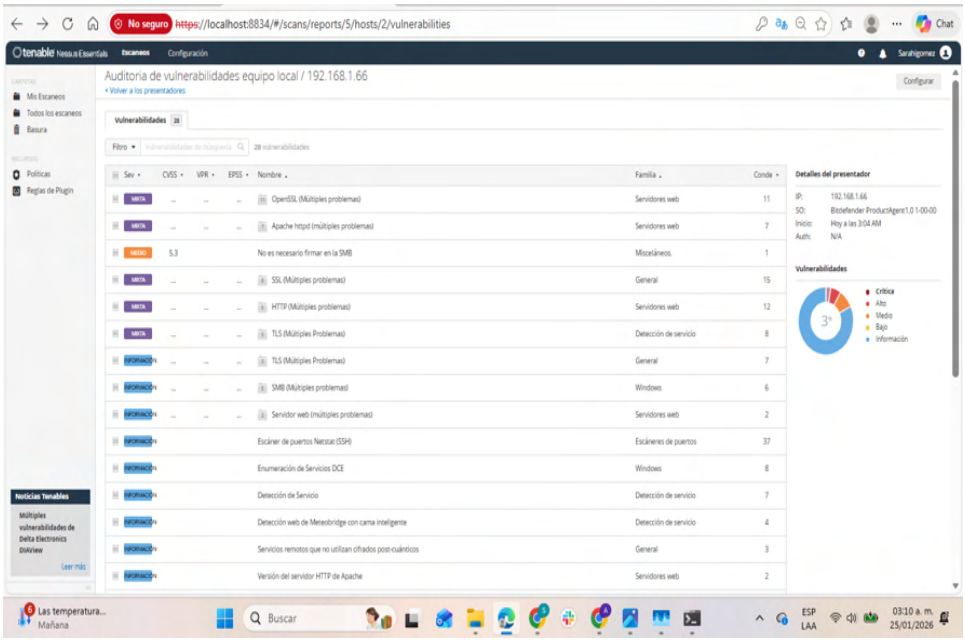


Nota: En esta sección se despliega una lista más amplia de vulnerabilidades relacionadas con OpenSSL, Apache HTTP, SSL, HTTP y TLS. Estas categorías corresponden a servicios web y protocolos de cifrado.

La presencia de múltiples problemas en estos componentes sugiere que el equipo cuenta con servicios activos que podrían estar desactualizados o configurados de forma insegura, en la seguridad informática, esto es relevante porque vulnerabilidades en OpenSSL o TLS son frecuentemente explotadas para comprometer comunicaciones cifradas y obtener datos sensibles.

Figura 44

Continuación del listado de hallazgos informativos

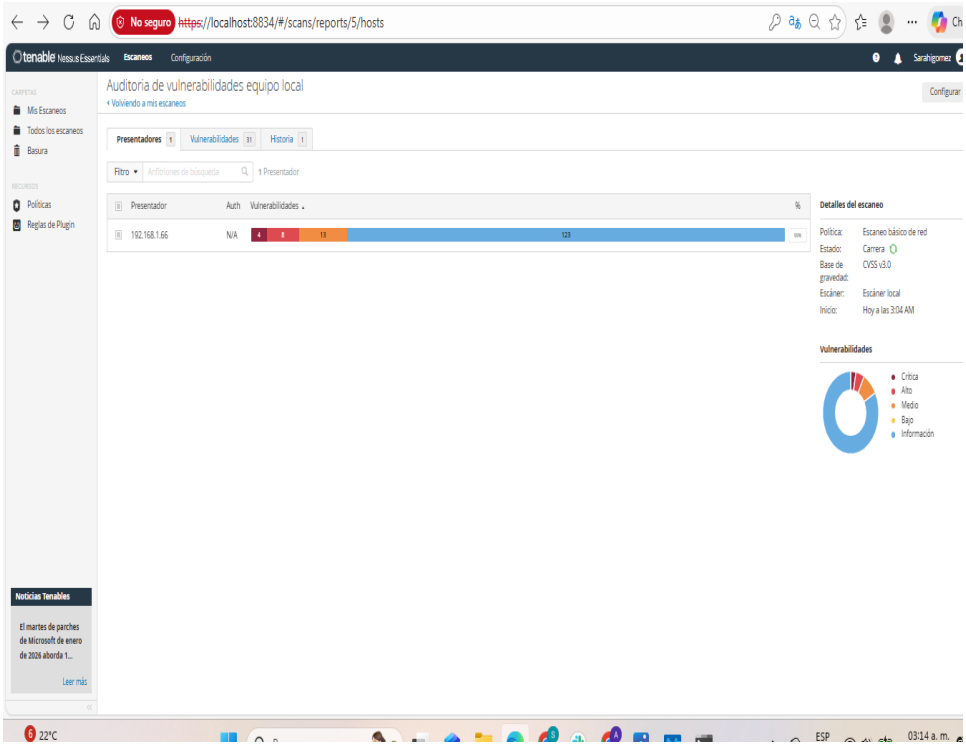


Nota: Aquí se observan vulnerabilidades informativas relacionadas con la detección de servicios, versiones de servidores web, protocolos soportados y servicios remotos activos.

Aunque no se clasifican como graves, proporcionan a un posible atacante información valiosa sobre el sistema, conocida como reconocimiento o fingerprinting, en ciberseguridad, esta fase de reconocimiento es crucial para planear ataques más sofisticados, por lo que reducir la exposición de información es una práctica recomendada.

Figura 45

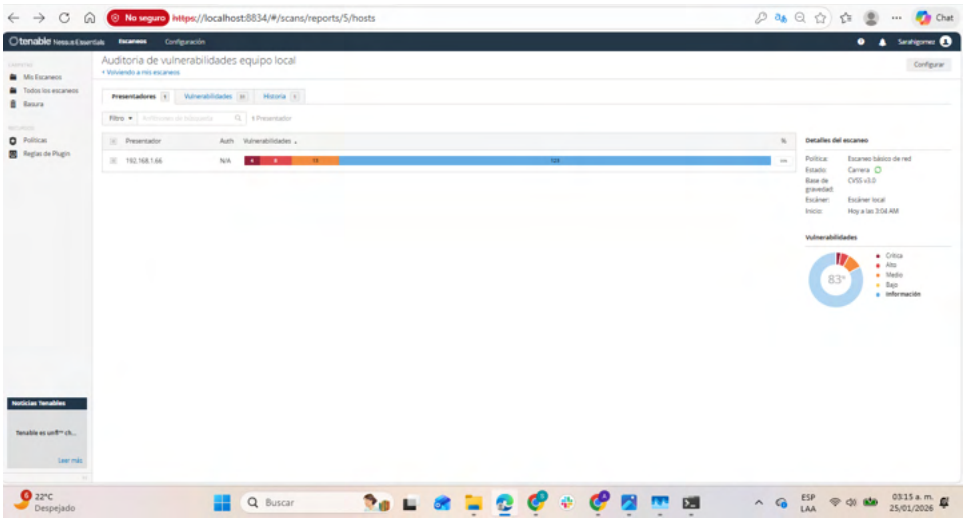
Identificación del sistema operativo y servicios activos



Nota: Esta imagen muestra cómo Nessus logra identificar el sistema operativo, servicios instalados y huellas del sistema, esto confirma que el escaneo fue efectivo en la enumeración del entorno del equipo, desde el punto de vista de seguridad, permitir que herramientas externas detecten con facilidad el sistema operativo puede facilitar ataques dirigidos, ya que los atacantes pueden buscar vulnerabilidades específicas para esa versión.

Figura 46

Información adicional de red y servicios remotos

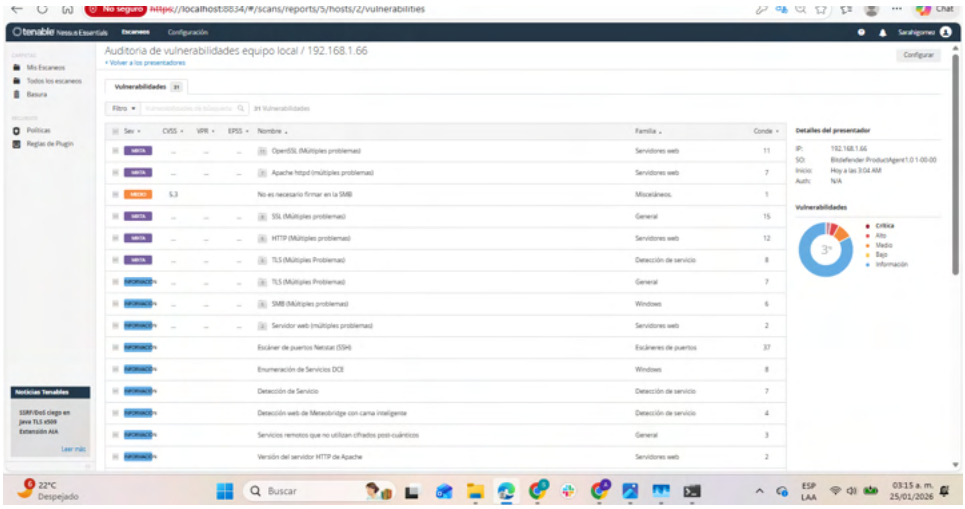


Nota: En esta captura se detallan servicios como PostgreSQL, certificados SSL y políticas de transporte seguro (HSTS), estos elementos indican que el equipo tiene componentes relacionados con servicios web y bases de datos.

Aunque se muestran como informativos, un mal manejo de certificados o configuraciones incorrectas de seguridad de transporte puede derivar en brechas de seguridad importantes, como ataques de suplantación o interceptación de tráfico cifrado.

Figura 47

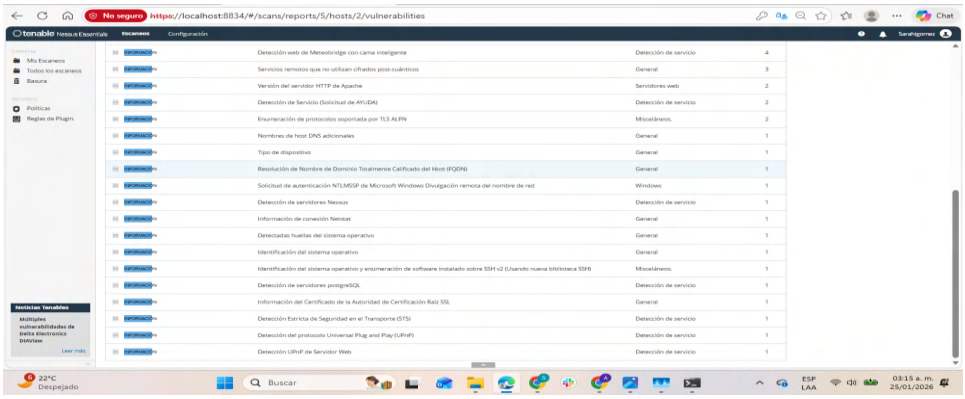
Detección de protocolos y dispositivos conectados



Nota: Aquí Nessus detecta protocolos como UPnP y otros servicios de red activos. UPnP, aunque facilita la conexión automática de dispositivos, es considerado un riesgo potencial, ya que ha sido explotado en múltiples ataques para abrir puertos sin autorización del usuario, en términos de seguridad informática, se recomienda deshabilitar UPnP si no es estrictamente necesario para reducir la exposición de la red.

Figura 48

Vista consolidada del estado de vulnerabilidades del host



Nota: Finalmente, esta imagen muestra nuevamente el resumen general del host con su distribución de vulnerabilidades en el gráfico circular, se observa que el mayor porcentaje corresponde a hallazgos informativos, con una pequeña fracción de vulnerabilidades medias y algunas altas o críticas dependiendo del momento del escaneo, esta visualización permite comprender rápidamente el nivel de riesgo del sistema. Desde una perspectiva de seguridad, aunque no se presenta una situación de alto peligro inmediato, sí se evidencia la necesidad de aplicar actualizaciones, reforzar configuraciones de red y deshabilitar servicios innecesarios para reducir la superficie de ataque.

En esta parte del escaneo realizado con Nessus Essentials demuestra que el equipo local presenta principalmente exposiciones informativas relacionadas con servicios activos, protocolos de red y configuraciones visibles desde la red, aunque las vulnerabilidades críticas son mínimas, la presencia de problemas en SMB, SSL, HTTP y TLS indica riesgos potenciales de interceptación, explotación remota y recopilación de información por parte de atacantes.

Recomendaciones de mitigación:

• Habilitar firma de mensajes en SMB

• Actualizar OpenSSL, Apache y servicios web

• Deshabilitar protocolos innecesarios como UPnP

• Limitar servicios expuestos a la red

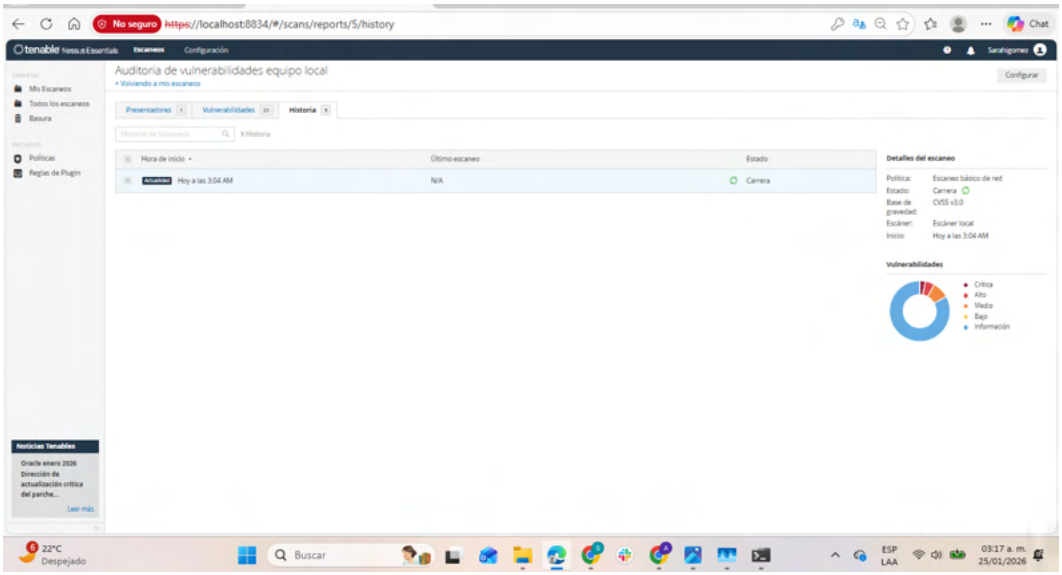
• Mantener parches de seguridad actualizados

• Configurar firewalls para restringir accesos

Reporte:

Figura 49

Estado del escaneo en ejecución dentro del historial de Nessus

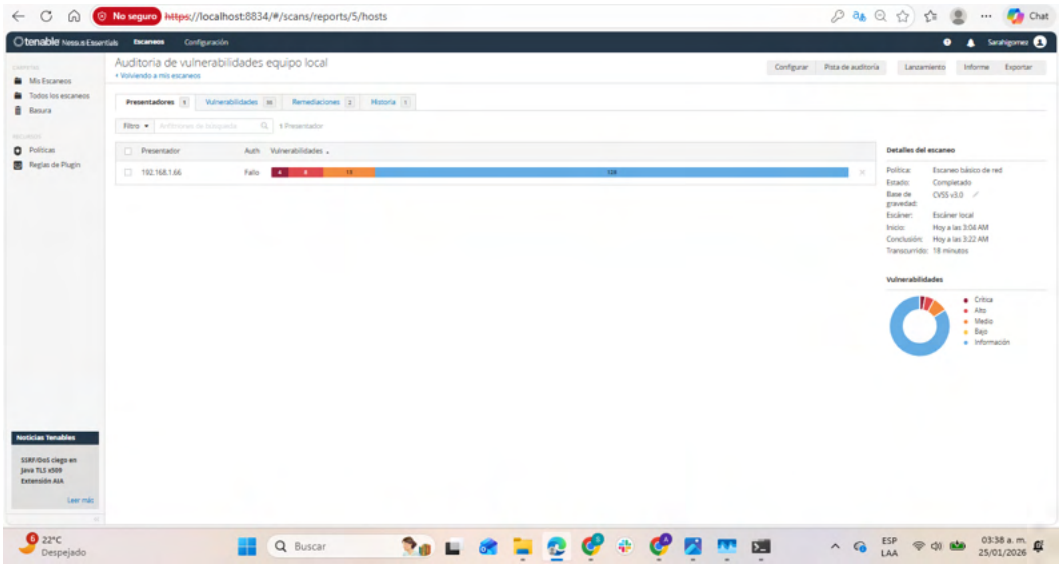


Nota: En esta captura se observa el historial del escaneo de vulnerabilidades donde el estado aparece como “Carrera”, indicando que el análisis aún se encuentra en proceso. Desde el punto de vista de seguridad informática, esta fase es crítica, ya que es cuando Nessus realiza la enumeración de servicios, detección de puertos abiertos, análisis de configuraciones y verificación de posibles vulnerabilidades conocidas.

La presencia del ícono verde refleja que el escaneo está activo y funcionando correctamente. El horario de inicio (3:04 AM) permite documentar la duración del análisis, lo cual es importante para auditorías técnicas.

Figura 50

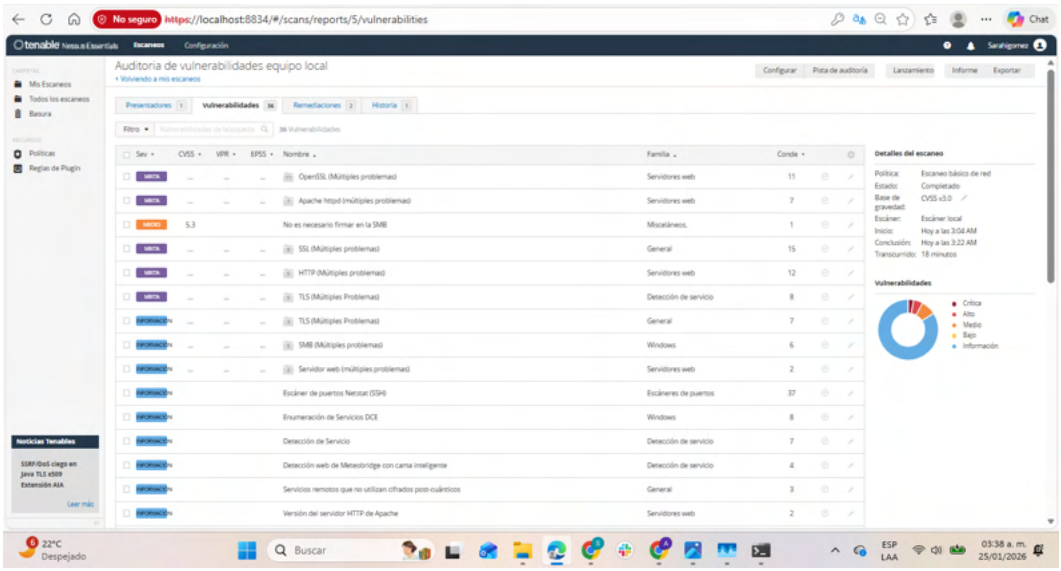
Sección de historial con escaneo completado:



Nota: Aquí se muestra el mismo escaneo una vez que ha finalizado, indicando el estado como “Completado” y mostrando la hora de conclusión (3:22 AM), esto permite confirmar que el proceso de auditoría se realizó exitosamente en un lapso aproximado de 18 minutos.

Figura 51

Listado general de vulnerabilidades detectadas en el equipo local

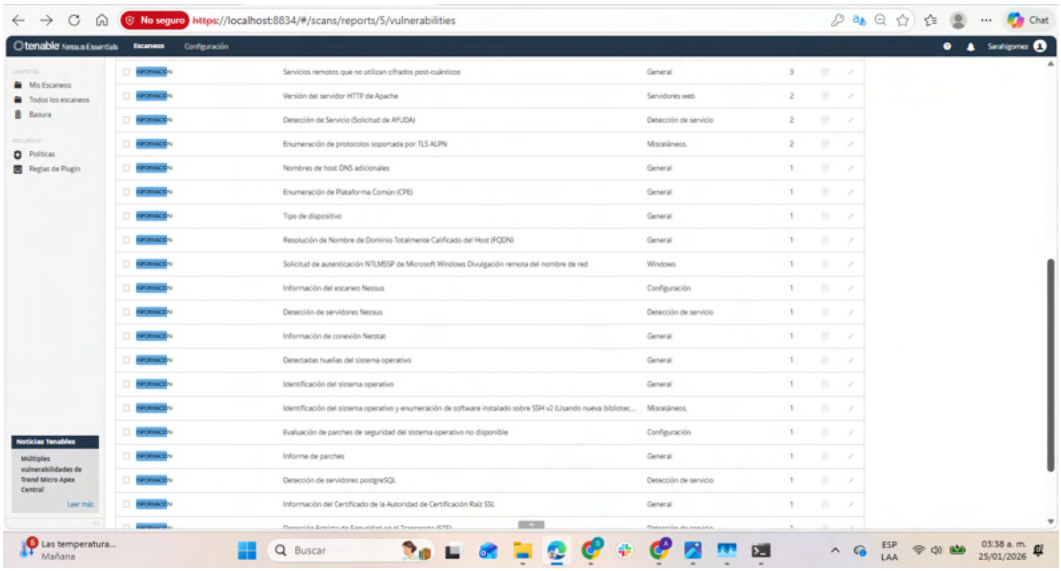


Nota: En esta captura se presenta la vista principal de la sección de vulnerabilidades dentro de Nessus Essentials, donde se muestran un total de 36 hallazgos clasificados por severidad y tipo, se observan múltiples vulnerabilidades relacionadas con OpenSSL, Apache HTTP, SSL, HTTP y TLS, así como una vulnerabilidad de nivel medio asociada al protocolo SMB que indica que no es necesario firmar las comunicaciones.

Desde el punto de vista de la seguridad informática, este listado es fundamental, ya que permite identificar qué servicios y componentes del sistema presentan debilidades conocidas, la repetición de problemas en tecnologías web y de cifrado sugiere que el equipo ejecuta servicios activos que pueden encontrarse desactualizados o mal configurados, este tipo de exposición representa un riesgo potencial de ataques remotos, interceptación de información y explotación de fallos conocidos, por lo que resulta indispensable aplicar parches de seguridad y revisar configuraciones de red.

Figura 52

Continuación del listado de vulnerabilidades informativas detectadas por Nessus:

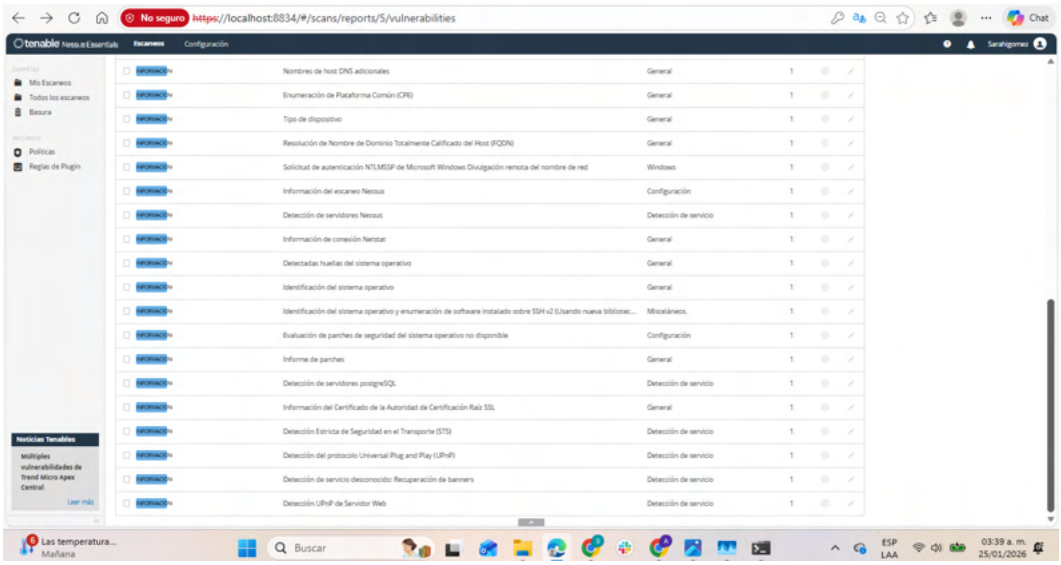


Nota: En esta imagen se observa la continuación del listado de vulnerabilidades clasificadas como informativas, incluyendo detección de servicios remotos, identificación del sistema operativo, enumeración de protocolos soportados, información de conexión Netstat, detección de servidores PostgreSQL, certificados SSL y configuraciones de transporte seguro. Aunque estas no se consideran fallos críticos, desde la perspectiva de la ciberseguridad representan una fase clave de reconocimiento o fingerprinting del sistema.

La exposición de este tipo de información facilita que un atacante pueda construir un perfil detallado del equipo, identificar versiones de software y seleccionar técnicas de ataque específicas, en auditorías de seguridad, este tipo de hallazgos demuestra que el sistema es altamente visible desde la red, lo que incrementa la superficie de ataque. Por ello, se recomienda minimizar la divulgación de información del sistema, restringir servicios innecesarios y reforzar controles de red.

Figura 53

Vista de hosts analizados y resumen de vulnerabilidades:



Nota: En esta imagen se observa una parte más profunda del listado de vulnerabilidades clasificadas como informativas dentro de Nessus Essentials. Se incluyen hallazgos como nombres adicionales de host DNS, enumeración de la plataforma común (CPE), identificación del tipo de dispositivo, resolución de nombres de dominio completamente calificados (FQDN), información del escaneo Nessus, detección de servidores Nessus, información de conexiones Netstat, huellas del sistema operativo e identificación del mismo.

Además, se muestran resultados relacionados con evaluaciones de parches del sistema operativo, informes de parches, detección de servidores PostgreSQL, información de certificados de autoridades raíz SSL, detección de políticas de seguridad de transporte (STS) y protocolos como UPnP.

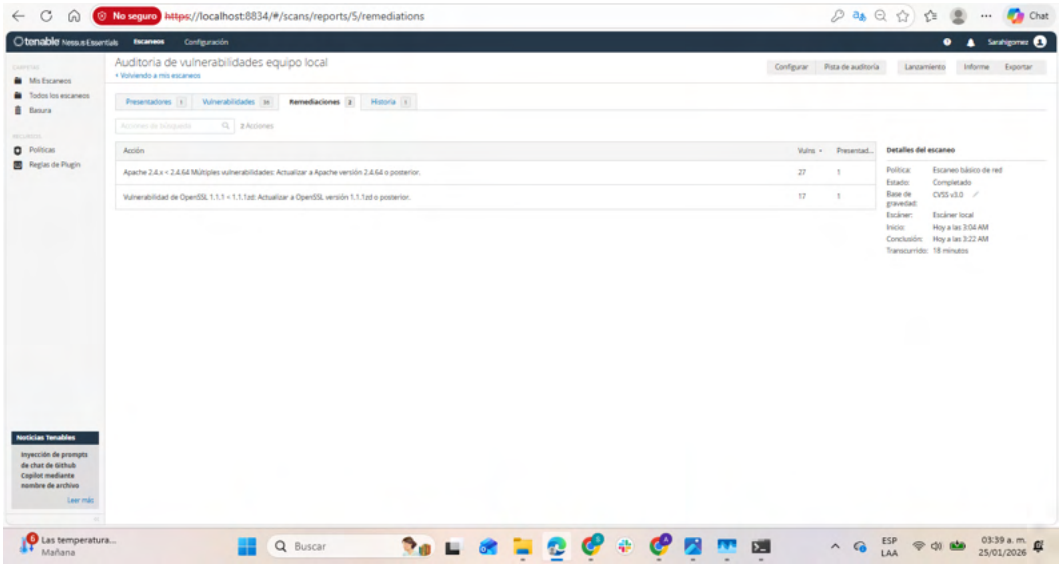
Desde la perspectiva de la seguridad informática, aunque estos hallazgos no representan vulnerabilidades explotables directamente, son extremadamente relevantes en la fase de reconocimiento de un ataque.

La enumeración detallada del sistema operativo, servicios activos, certificados y protocolos permite que un atacante obtenga un mapa completo del entorno del sistema analizado, esto facilita la selección de vectores de ataque específicos dirigidos a versiones concretas de software o configuraciones detectadas, la detección de UPnP, por ejemplo, es especialmente importante, ya que este protocolo ha sido históricamente utilizado para abrir puertos automáticamente, lo que puede generar accesos no autorizados desde redes externas.

En un contexto de auditoría de seguridad, este tipo de información demuestra que el sistema es altamente visible dentro de la red y que existen múltiples puntos potenciales de exposición, por ello, se recomienda deshabilitar servicios innecesarios, restringir la divulgación de información del sistema, mantener certificados actualizados y aplicar controles de firewall que limiten la accesibilidad a servicios críticos.

Figura 54

Sección de remediaciones recomendadas por Nessus Essentials



Nota: Se muestra el listado completo de vulnerabilidades organizadas por categoría y severidad y en esta imagen se observa la pestaña de “Remediaciones” dentro del reporte de

auditoría de vulnerabilidades del equipo local, donde Nessus Essentials presenta acciones concretas para corregir los problemas detectados durante el escaneo, se muestran principalmente dos recomendaciones críticas: la actualización del servidor Apache HTTP a una versión superior a la 2.4.64 y la actualización de la biblioteca OpenSSL a una versión posterior a la 1.1.1zd. cada una de estas acciones está asociada con un número considerable de vulnerabilidades, lo que indica que múltiples fallos de seguridad se originan en versiones desactualizadas de estos componentes.

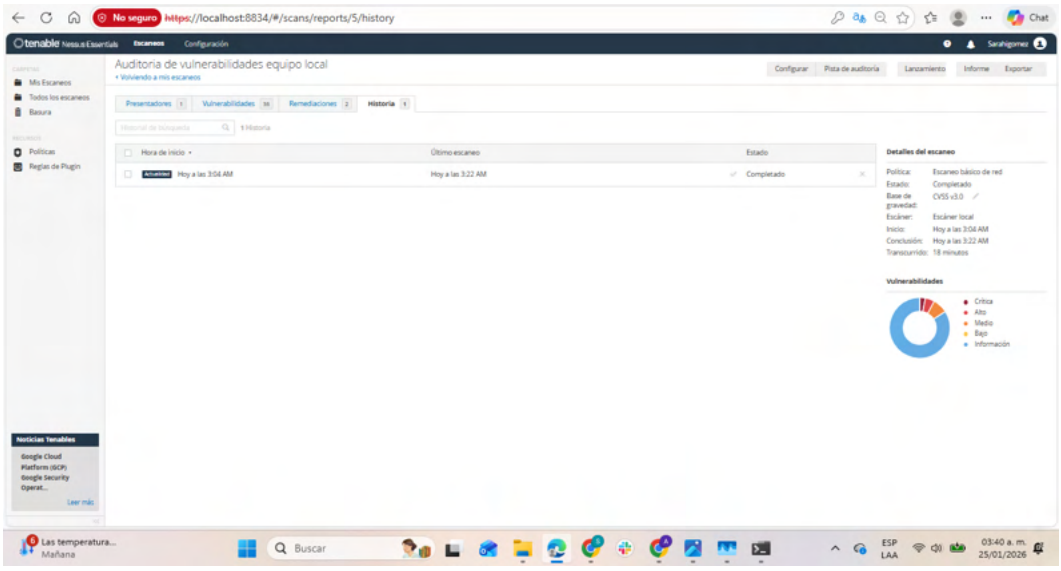
Desde el enfoque de la seguridad informática, esta sección es de suma importancia, ya que transforma los hallazgos técnicos en medidas prácticas de mitigación. Apache HTTP y OpenSSL son componentes fundamentales en muchos sistemas que manejan comunicaciones web y cifrado de datos, cuando estas herramientas presentan vulnerabilidades, los atacantes pueden explotar fallos para ejecutar código remoto, interceptar comunicaciones cifradas, acceder a información sensible o comprometer completamente el sistema, por ello, mantener estos servicios actualizados es una de las mejores prácticas más básicas y efectivas en ciberseguridad.

Además, el hecho de que Nessus agrupe múltiples vulnerabilidades bajo una sola acción de remediación permite priorizar esfuerzos de seguridad de manera eficiente, en lugar de corregir cada fallo individualmente, una simple actualización puede eliminar decenas de riesgos potenciales, esto demuestra cómo una mala gestión de actualizaciones puede incrementar considerablemente la superficie de ataque del sistema.

En un contexto de auditoría profesional, esta sección sirve como guía estratégica para fortalecer la seguridad del equipo, indicando claramente qué componentes requieren intervención inmediata, la implementación de estas remediaciones reduciría significativamente el nivel de exposición del sistema ante amenazas externas y mejoraría su postura general de seguridad.

Figura 55

Historial del escaneo de vulnerabilidades con estado completado



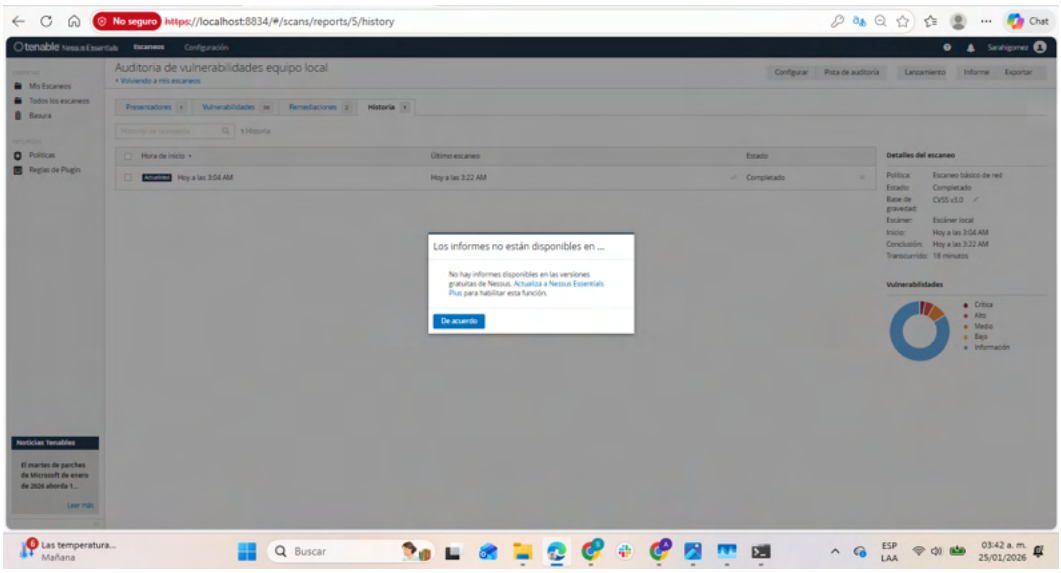
Nota: En esta captura se observa el historial del proceso de auditoría de vulnerabilidades realizado con Nessus Essentials, donde el escaneo iniciado a las 3:04 AM aparece con estado "Completado" a las 3:22 AM, indicando que el análisis concluyó de forma exitosa tras un tiempo aproximado de 18 minutos, este intervalo refleja que Nessus ejecutó una revisión detallada del sistema, incluyendo la detección de servicios activos, enumeración de puertos abiertos, análisis de configuraciones de red y verificación de vulnerabilidades conocidas.

Desde el punto de vista de la seguridad informática, el registro del historial es una herramienta fundamental en auditorías técnicas, ya que permite confirmar que los procesos se realizaron correctamente y proporciona evidencia temporal del análisis efectuado, además, contar con datos de inicio, finalización y duración del escaneo facilita la comparación de resultados en auditorías futuras, ayudando a evaluar si las acciones de mitigación implementadas reducen el número de vulnerabilidades detectadas.

El estado de “Completado” garantiza que los resultados obtenidos son confiables y representan una evaluación completa del host analizado, en un contexto profesional, esta información es clave para validar informes de seguridad, demostrar cumplimiento de procesos de auditoría y asegurar que no existieron interrupciones que pudieran afectar la precisión de los hallazgos.

Figura 56

Advertencia sobre la indisponibilidad de informes en Nessus Essentials



Nota: En esta imagen se observa una ventana emergente dentro de la plataforma Nessus Essentials indicando que la generación de informes no se encuentra disponible en la versión gratuita del software, sugiriendo la actualización a Nessus Essentials Plus para habilitar esta funcionalidad, este mensaje evidencia una de las principales limitaciones de las versiones gratuitas de herramientas profesionales de auditoría de seguridad, ya que los reportes automatizados son fundamentales para documentar formalmente los hallazgos, presentar resultados técnicos y realizar seguimientos de vulnerabilidades a lo largo del tiempo.

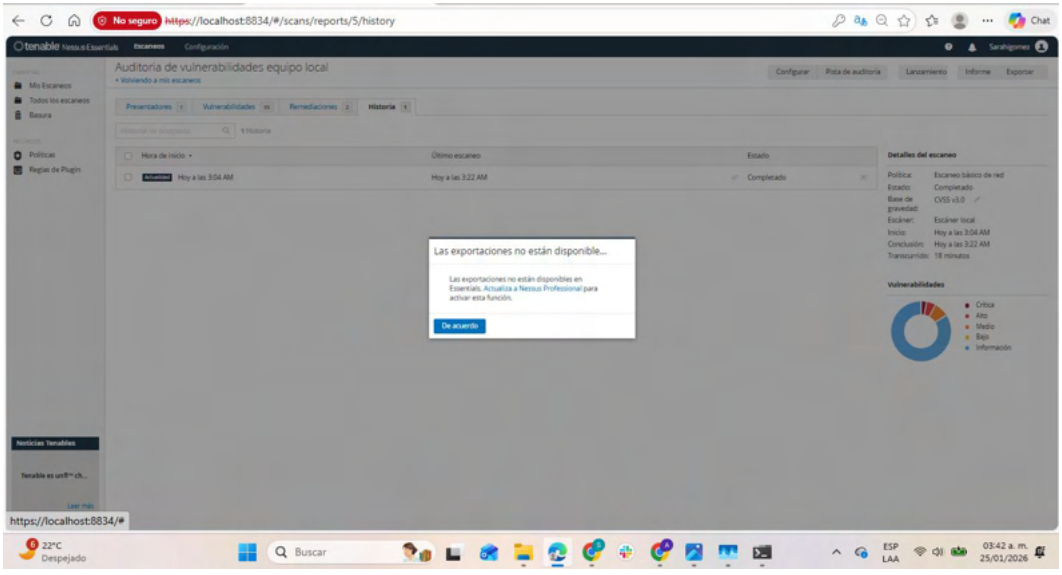
Desde el enfoque de la seguridad informática, la generación de informes estructurados

permite consolidar la información de los escaneos, clasificar riesgos, priorizar vulnerabilidades y comunicar de forma clara los resultados a administradores de sistemas, equipos de TI o responsables de seguridad. La ausencia de esta función obliga al usuario a realizar un proceso manual de recopilación de evidencias, como capturas de pantalla y análisis escritos, tal como se está desarrollando en esta auditoría académica.

Asimismo, este tipo de limitaciones demuestra la importancia de las versiones profesionales en entornos empresariales, donde la automatización de reportes reduce errores humanos, facilita auditorías periódicas y permite cumplir con normativas de seguridad y estándares internacionales, sin embargo, aunque la función no esté habilitada, la interfaz de Nessus continúa proporcionando información detallada y válida para el análisis de vulnerabilidades, permitiendo identificar riesgos y establecer medidas de mitigación.

Figura 57

Restricción de exportación de resultados en Nessus Essentials



Nota: En esta captura se observa una ventana emergente generada por Nessus Essentials que informa al usuario que la función de exportación de resultados no se encuentra disponible en

la versión gratuita de la herramienta, recomendando la actualización a Nessus Professional para habilitar esta característica, esta limitación impide descargar los datos del escaneo en formatos estructurados como CSV, XML o archivos compatibles con otras plataformas de análisis de seguridad.

Desde el enfoque de la seguridad informática, la exportación de resultados es una funcionalidad clave dentro de los procesos de auditoría, ya que permite realizar análisis más profundos, correlacionar vulnerabilidades con otras herramientas de monitoreo, generar reportes personalizados y conservar evidencia técnica para revisiones futuras. La ausencia de esta opción obliga al analista a trabajar directamente desde la interfaz web, interpretando manualmente cada hallazgo.

Esta restricción demuestra una diferencia importante entre las versiones gratuitas y profesionales de herramientas de ciberseguridad, donde las ediciones completas están orientadas a entornos empresariales que requieren automatización, integración con sistemas de gestión de riesgos y generación de reportes técnicos avanzados, sin embargo, aunque Nessus Essentials no permite exportar los datos, sigue proporcionando información suficiente para identificar vulnerabilidades, evaluar niveles de riesgo y proponer acciones de mitigación de forma manual.

En el contexto de esta auditoría académica, esta evidencia confirma que se utilizó una herramienta real de evaluación de vulnerabilidades bajo condiciones auténticas de uso, enfrentando limitaciones comunes en entornos gratuitos, a pesar de estas restricciones, los resultados obtenidos siguen siendo válidos para el análisis de la postura de seguridad del sistema, demostrando cómo incluso versiones básicas de herramientas profesionales pueden contribuir significativamente a la detección temprana de riesgos y a la mejora de la seguridad informática del equipo analizado.

Análisis e Identificación de Mejoras

Con base en los resultados obtenidos durante la auditoría de vulnerabilidades realizada mediante la herramienta Nessus Essentials, se identificó que el equipo analizado presenta principalmente incidencias clasificadas como informativas, así como un conjunto reducido de vulnerabilidades de nivel medio, aunque no se detectaron amenazas críticas inmediatas, los hallazgos evidencian una alta exposición del sistema en la red, debido a la presencia de múltiples servicios activos, protocolos visibles y configuraciones que pueden ser aprovechadas por posibles atacantes.

Entre las principales vulnerabilidades encontradas se destacan aquellas relacionadas con componentes de comunicación web y cifrado, tales como OpenSSL, Apache HTTP, SSL, HTTP y TLS. La repetición de incidencias en estos servicios sugiere que el sistema ejecuta versiones desactualizadas o con configuraciones inseguras, lo cual representa un riesgo significativo para la integridad, confidencialidad y disponibilidad de la información, asimismo, se detectó una vulnerabilidad de nivel medio asociada al protocolo SMB, la cual indica que las comunicaciones no requieren firma digital, facilitando posibles ataques de intermediario (Man-in-the-Middle).

Adicionalmente, la auditoría reveló una gran cantidad de hallazgos informativos relacionados con la detección del sistema operativo, servicios remotos, protocolos de red, certificados SSL, servidores de bases de datos y configuraciones visibles desde la red, aunque estas incidencias no constituyen fallos explotables de manera directa, proporcionan información valiosa que puede ser utilizada durante la fase de reconocimiento de un ataque, aumentando considerablemente la superficie de ataque del sistema analizado.

Como resultado de este análisis, se identifican diversas áreas de mejora para fortalecer la seguridad del equipo:

En primer lugar, se recomienda implementar una política de actualización periódica de software, especialmente en servicios críticos como Apache HTTP y OpenSSL, con el fin de corregir vulnerabilidades conocidas y reducir la exposición ante ataques remotos.

En segundo lugar, es fundamental revisar y reforzar las configuraciones de red, deshabilitando servicios innecesarios y limitando la visibilidad del sistema para minimizar la recopilación de información por parte de posibles atacantes.

Asimismo, se sugiere habilitar mecanismos de seguridad adicionales, como la firma de mensajes en el protocolo SMB, el uso de firewalls para restringir accesos no autorizados y la aplicación de controles de monitoreo continuo que permitan detectar actividades sospechosas de forma temprana. La implementación de estas medidas contribuirá significativamente a mejorar la postura de seguridad del sistema y a prevenir incidentes futuros.

En conclusión, aunque el equipo no presenta vulnerabilidades críticas de alto impacto inmediato, los resultados obtenidos demuestran la importancia de realizar auditorías periódicas de seguridad, ya que incluso sistemas aparentemente seguros pueden presentar múltiples puntos de exposición. La correcta interpretación de los hallazgos y la aplicación de las mejoras propuestas permitirán reducir riesgos, fortalecer la protección de la información y promover una cultura de seguridad informática preventiva.

Conclusión:

La auditoría de vulnerabilidades realizada mediante la herramienta Nessus Essentials permitió identificar de manera efectiva los riesgos de seguridad presentes en el equipo de cómputo analizado, demostrando la importancia de implementar procesos de evaluación continua para prevenir ataques de acceso no autorizado, a lo largo del desarrollo del proyecto se evidenció cómo, mediante una correcta instalación, configuración y ejecución del escaneo de red, es posible detectar tanto vulnerabilidades técnicas como exposiciones informativas que incrementan la superficie de ataque del sistema.

Los resultados obtenidos mostraron principalmente incidencias de carácter informativo, relacionadas con servicios activos, protocolos visibles y configuraciones detectables desde la red, así como un conjunto reducido de vulnerabilidades de nivel medio asociadas a componentes críticos como OpenSSL, Apache HTTP y el protocolo SMB, aunque no se identificaron amenazas críticas inmediatas, estos hallazgos reflejan que el sistema presenta múltiples puntos potenciales de exposición que podrían ser aprovechados por atacantes si no se gestionan adecuadamente.

El análisis realizado permitió comprender que muchas de las vulnerabilidades detectadas se originan en versiones desactualizadas de software y en configuraciones de red poco restrictivas, lo que resalta la importancia de mantener políticas de actualización periódica, control de servicios expuestos y aplicación de medidas preventivas como firewalls, firma de comunicaciones y monitoreo constante, asimismo, la gran cantidad de información revelada por el escaneo evidencia cómo incluso sistemas comunes pueden proporcionar datos valiosos para la fase de reconocimiento de un ataque.

En conclusión, este proyecto demuestra que las auditorías de seguridad informática son una herramienta fundamental para fortalecer la protección de los sistemas, ya que permiten identificar riesgos, analizar su impacto y establecer acciones de mitigación efectivas, la correcta interpretación de los resultados obtenidos y la implementación de las mejoras propuestas contribuirán a reducir la exposición del equipo ante amenazas externas, promoviendo una postura de seguridad más sólida y preventiva frente a posibles ataques de acceso.

Además, la adquisición de este tipo de conocimientos resulta de gran importancia tanto en el ámbito laboral como en la vida cotidiana, en el entorno profesional, las habilidades desarrolladas durante esta auditoría permiten desempeñar funciones relacionadas con la seguridad de la información, como la evaluación de sistemas, detección de vulnerabilidades, análisis de riesgos y aplicación de medidas preventivas, competencias altamente demandadas en áreas de tecnología, redes y ciberseguridad, empresas e instituciones requieren constantemente personal capacitado para proteger sus sistemas ante amenazas cada vez más frecuentes y sofisticadas.

En la vida cotidiana, estos conocimientos permiten a los usuarios comprender la importancia de mantener sus equipos actualizados, proteger redes domésticas, reconocer configuraciones inseguras y evitar prácticas que puedan comprometer su información personal, por ejemplo, identificar servicios innecesarios activos, aplicar actualizaciones de seguridad o configurar correctamente el acceso a redes inalámbricas son acciones que contribuyen a reducir el riesgo de ataques comunes como intrusiones, robo de datos o infecciones de malware.

Durante el desarrollo del proyecto se adquirieron diversas habilidades técnicas y analíticas, tales como la instalación y configuración de herramientas de auditoría de seguridad, la identificación de direcciones IP y servicios de red, la interpretación de gráficos de

vulnerabilidades, el análisis de resultados técnicos y la propuesta de soluciones de mitigación, asimismo, se fortalecieron habilidades de documentación, análisis crítico y aplicación práctica de conceptos teóricos de seguridad informática.

En conjunto, este proyecto no solo permitió comprender el funcionamiento de una herramienta profesional de auditoría de vulnerabilidades, sino que también fomentó una visión preventiva de la seguridad informática, preparando al estudiante para enfrentar retos reales en el ámbito tecnológico y promoviendo buenas prácticas de protección de la información tanto a nivel profesional como personal.

Referencias:

Burgin, J. (2025, 29 mayo). *Vulnerability scanning: best practices & advanced detection*. Upwind | Cloud Security Happens At Runtime. https://www.upwind.io/glossary/what-is-vulnerability-scanning

Cilleruelo, C. (2025, 21 mayo). ¿Qué es Nessus y qué funciones tiene en ciberseguridad? - Guía 2026. *KeepCoding Bootcamps*. https://keepcoding.io/blog/que-es-nessus/

Cyberthreatsdefenders. (2024, 2 mayo). *Como usar Nessus Scan para escaneo de tu red y ver si algún equipo es vulnerable | Tutorial completo* [Vídeo]. YouTube. https://www.youtube.com/watch?v=2ZwAa5aYFuM

El Pingüino de Mario. (2022, 18 octubre). 💻 *CURSO DE HACKING ÉTICO - Detectar Vulnerabilidades AUTOMÁTICAMENTE con NESSUS #12* [Vídeo]. YouTube. https://www.youtube.com/watch?v=Vj3BpreFsR8

Escáner de vulnerabilidades Nessus:Solución de seguridad en la red. (s. f.). Tenable®. https://es-la.tenable.com/products/nessus

Juan. (2025a, abril 30). *Nessus: La Herramienta Esencial para la Detección y Gestión Proactiva de Vulnerabilidades en Ciberseguridad*. Cibersafety. https://cibersafety.com/nessus-herramienta-gestion-vulnerabilidades-ciberseguridad/

Juan. (2025b, abril 30). *Nessus: La Herramienta Esencial para la Detección y Gestión Proactiva de Vulnerabilidades en Ciberseguridad*. Cibersafety. https://cibersafety.com/nessus-herramienta-gestion-vulnerabilidades-ciberseguridad

Kosinski, M., & Forrest, A. (2025, 17 noviembre). Vulnerability Scanning. *¿Qué es el escaneo de vulnerabilidades? IBM*. https://www.ibm.com/think/topics/vulnerability-scanning

RINKU. (2025, 2 octubre). *Curso de CIBERSEGURIDAD desde cero 2026 COMPLETO* [Vídeo]. YouTube. https://www.youtube.com/watch?v=rctz_w5SB3A

Video conferencing, web conferencing, webinars, screen sharing. (s. f.). Zoom. https://academiaglobal-mx.zoom.us/rec/play/5poAPkbPraPJ6o6ZNb6dxkrHtEvTe0zX81pguCin5_MpUg36z1V7cvvg0Pi-Y6baW4cSXYs_yaqXFtF2.eRJkg0bQ5IA7OfFK?eagerLoadZvaPages=sidemenu.billing.plan_management&accessLevel=meeting&canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2FKoCbuyb1TyhMJEousd4xN7NpCfBlxAbrEKt_Py4lbIPmoHBxmf162V8vVB9DFlvm.VJwDwsugbUDNNyLo

Vulnerability assessment. (s. f.-a). Tenable®. https://www.tenable.com/source/vulnerability-assessment

Vulnerability assessment. (s. f.-b). Tenable®. https://www.tenable.com/source/vulnerability-assessment

Vulnerability Scanning Tools | OWASP Foundation. (s. f.). https://owasp.org/www-community/Vulnerability_Scanning_Tools

Wilson, A. (2025, 12 noviembre). *¿Cómo hacer un escaneo de red?* Tenable®. https://es-la.tenable.com/cybersecurity-guide/learn/network-scanning