Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad [2] – [Monitoreo de Red]

[Seguridad Informática II]

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Carlos Fco Estrada Salazar

Fecha: 03/Feb/2025

INDICE

GitHub Link:

INTRODUCCIÓN

En el contexto de la seguridad informática, el monitoreo de red es una práctica fundamental para la prevención de ataques cibernéticos y la detección temprana de posibles vulnerabilidades dentro de una infraestructura tecnológica. La actividad de monitoreo no solo permite identificar intentos de acceso no autorizado, sino que también contribuye a mantener la integridad, disponibilidad y confidencialidad de los sistemas y datos de una organización. A través de la implementación de herramientas especializadas, es posible auditar y supervisar en tiempo real el tráfico de la red, los dispositivos conectados, y el comportamiento de los usuarios, lo que facilita la toma de decisiones informadas para la mejora continua de la seguridad.

El objetivo principal de esta actividad es instalar y configurar un software de monitoreo de red para analizar el entorno tecnológico actual. Esto incluye la identificación de todos los dispositivos conectados, la recopilación de datos relevantes sobre su estado, y la generación de un reporte detallado que permita evaluar posibles riesgos. Además, se establecerá una programación de auditorías semanales para asegurar un control constante del sistema, hardware, software, licencias y red, promoviendo así una gestión proactiva de la seguridad.

Otro aspecto crucial de esta actividad es la gestión de bitácoras, las cuales deben ser almacenadas de manera segura, eliminadas de forma periódica e iniciadas nuevamente para facilitar la detección de cambios o actividades sospechosas desde el primer día de registro. Esta práctica es vital para mantener un historial actualizado que permita rastrear eventos de seguridad con precisión y rapidez.

En resumen, esta actividad proporcionará una visión integral del estado actual de la red, fomentará la implementación de mejores prácticas en la auditoría de sistemas y contribuirá significativamente a la robustez del entorno de seguridad de la organización.

DESCRIPCIÓN

El monitoreo de red es un proceso esencial en el ámbito de la seguridad informática, ya que permite identificar, prevenir y mitigar posibles amenazas que puedan comprometer la integridad, confidencialidad y disponibilidad de los sistemas de información. En el contexto de esta actividad, el objetivo es implementar técnicas de protección que ayuden a prevenir ataques de explotación y accesos no autorizados mediante auditorías y un monitoreo constante de la red.

Prevenir los ataques de acceso es fundamental, ya que estos pueden derivar en la pérdida de información crítica o la interrupción de servicios esenciales. Para ello, es necesario identificar los puntos vulnerables en la infraestructura de red y establecer mecanismos de control que permitan detectar intentos de intrusión en tiempo real. Asimismo, la prevención de accesos no autorizados a las redes contribuye a mantener la seguridad perimetral, evitando que actores malintencionados puedan comprometer los recursos internos.

Otro aspecto relevante es la validación de licencias de software y hardware, no solo por el cumplimiento de aspectos legales y regulatorios, sino también para garantizar que los sistemas operen de manera segura y eficiente. El control total y la auditoría semanal del sistema permiten mantener un registro actualizado de cualquier cambio o anomalía, facilitando la identificación de posibles brechas de seguridad.

El monitoreo completo de la red abarca la supervisión del tráfico de datos, la identificación de dispositivos conectados y el análisis de patrones de comportamiento inusuales. La gestión de bitácoras es crucial, ya que proporciona un historial detallado de eventos que puede ser utilizado para la investigación forense en caso de incidentes de seguridad. La eliminación y creación de nuevas bitácoras facilita la detección de cambios desde el primer día de registro, lo que mejora la capacidad de respuesta ante amenazas emergentes.

En conclusión, esta actividad no solo fortalece la comprensión de los principios básicos de la seguridad informática, sino que también desarrolla habilidades prácticas en la implementación de medidas de protección efectivas, contribuyendo así a un entorno tecnológico más seguro y resiliente.

JUSTIFICACIÓN

El uso de soluciones de monitoreo de red es fundamental para garantizar la seguridad de los sistemas informáticos en cualquier organización. En el contexto de esta actividad, la implementación de un software de monitoreo permite identificar de manera proactiva posibles amenazas y vulnerabilidades que podrían comprometer la integridad, confidencialidad y disponibilidad de la información. Esta solución no solo detecta accesos no autorizados, sino que también contribuye a prevenir ataques de explotación mediante la supervisión continua del tráfico de red y los dispositivos conectados.

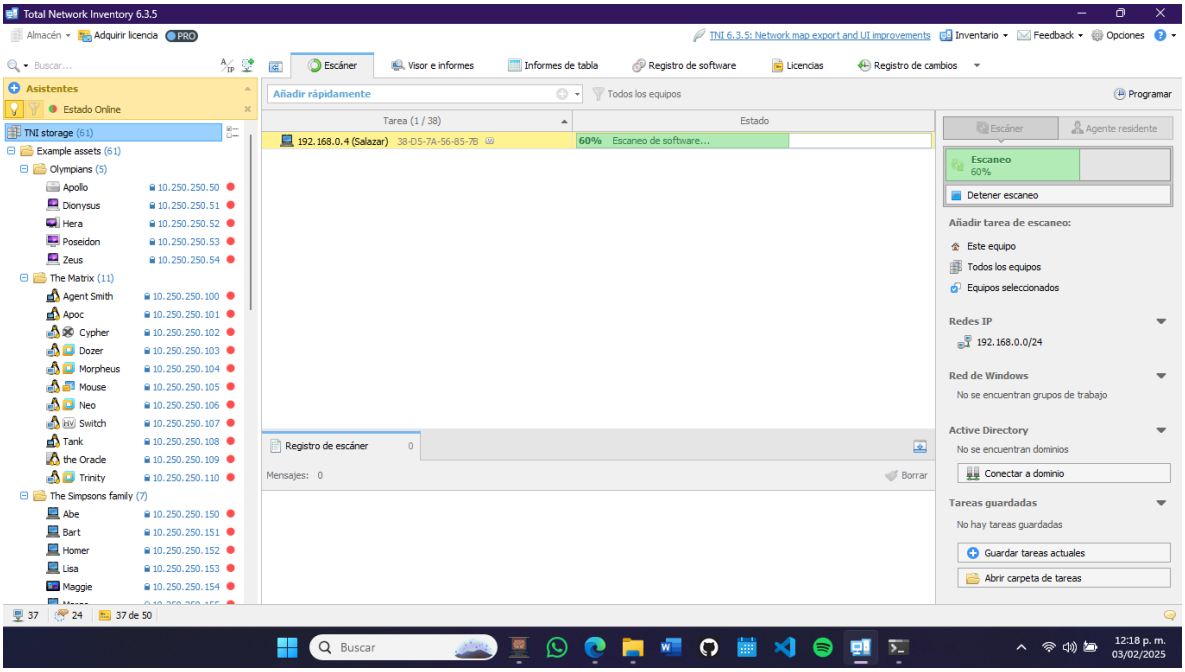
Una de las razones principales para emplear este tipo de solución es la capacidad de mantener un control total sobre el sistema, hardware, software, licencias y red. La auditoría semanal programada asegura que cualquier cambio en la infraestructura sea identificado y evaluado, lo que facilita la toma de decisiones informadas para la mitigación de riesgos. Además, la validación de licencias y la verificación de la legalidad de los recursos utilizados ayudan a cumplir con los aspectos legales y regulatorios, evitando posibles sanciones y garantizando un entorno de trabajo seguro.

El monitoreo completo de la red permite detectar patrones de comportamiento inusuales que podrían indicar la presencia de intrusos o actividades maliciosas. La generación y gestión de bitácoras es otra ventaja clave, ya que proporciona un registro detallado de eventos que facilita el análisis forense en caso de incidentes de seguridad. El proceso de eliminar y reiniciar bitácoras periódicamente ayuda a identificar cambios desde el primer día de registro, mejorando la capacidad de respuesta ante nuevas amenazas.

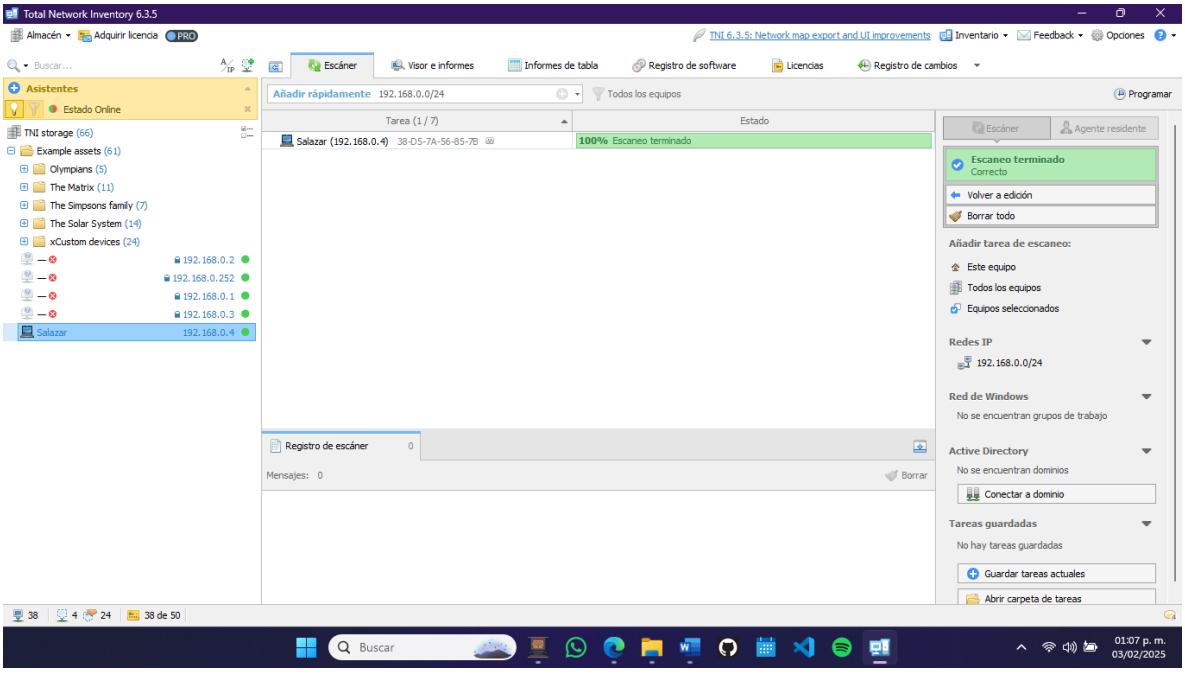
En conclusión, emplear soluciones de monitoreo de red no solo fortalece la postura de seguridad de la organización, sino que también promueve una cultura de vigilancia y mejora continua. Esta práctica es esencial para proteger los activos críticos, garantizar la continuidad del negocio y mantener la confianza de los usuarios y clientes en la integridad de los sistemas de información.

DESARROLLO

Resultado de Escaneo

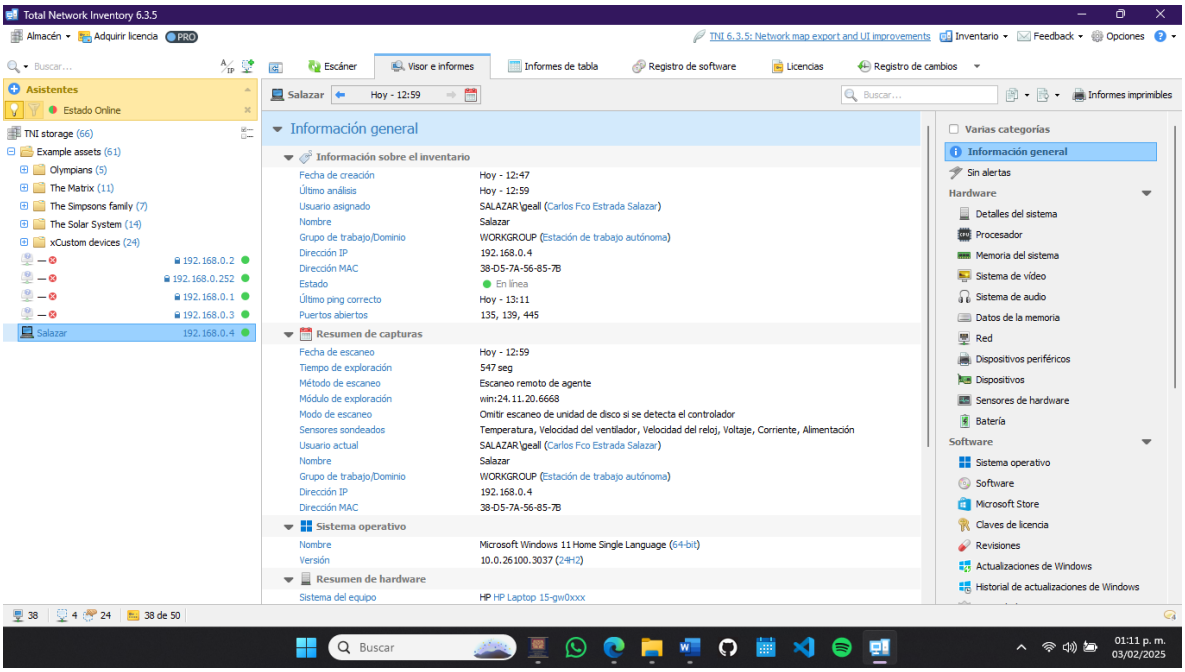


Escaneo de red

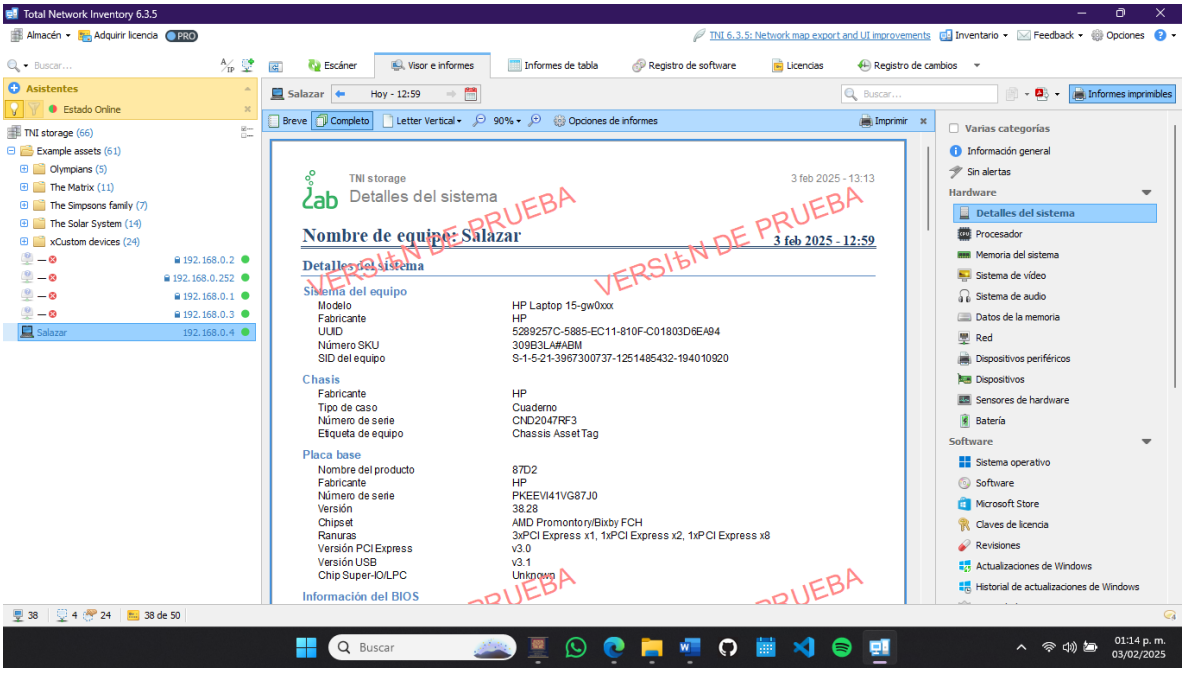


Escaneo terminado

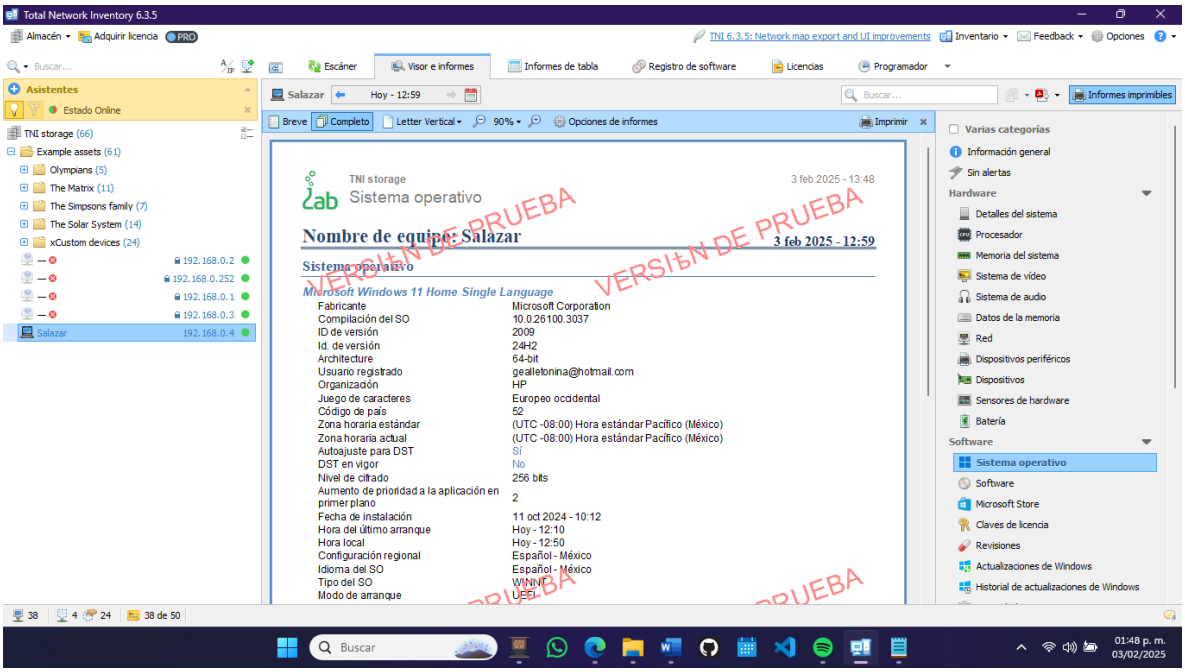
Reporte



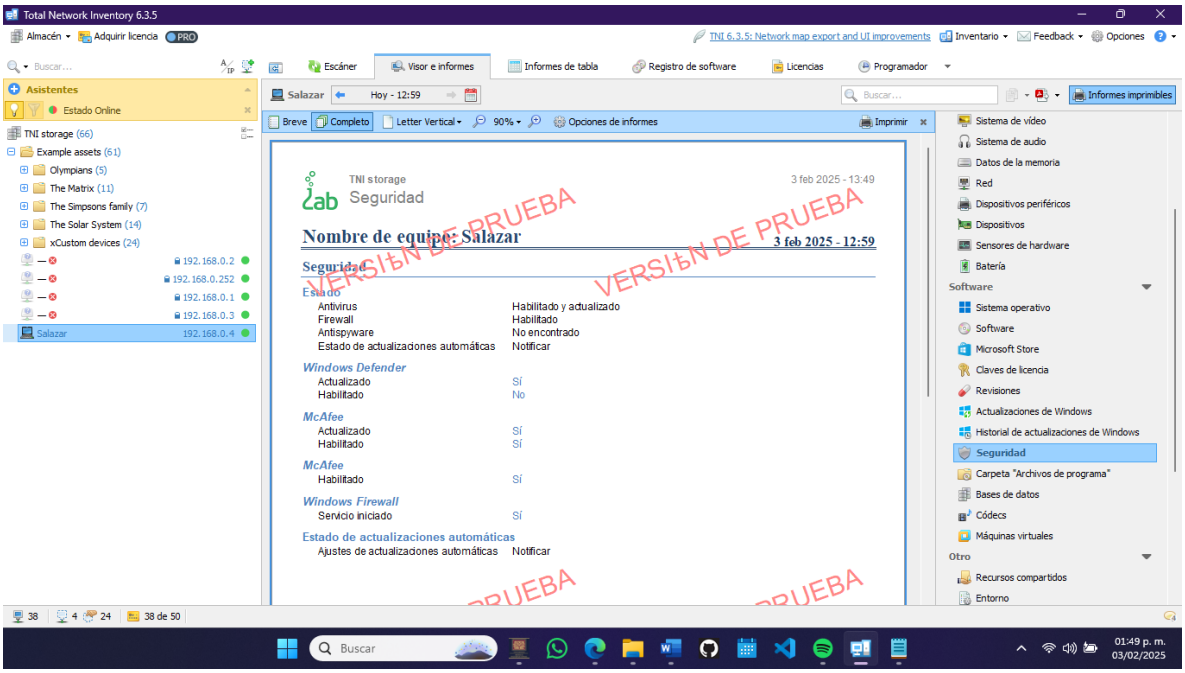
Presento el reporte del escaneo de mi equipo



Reporte de Estado de sistema

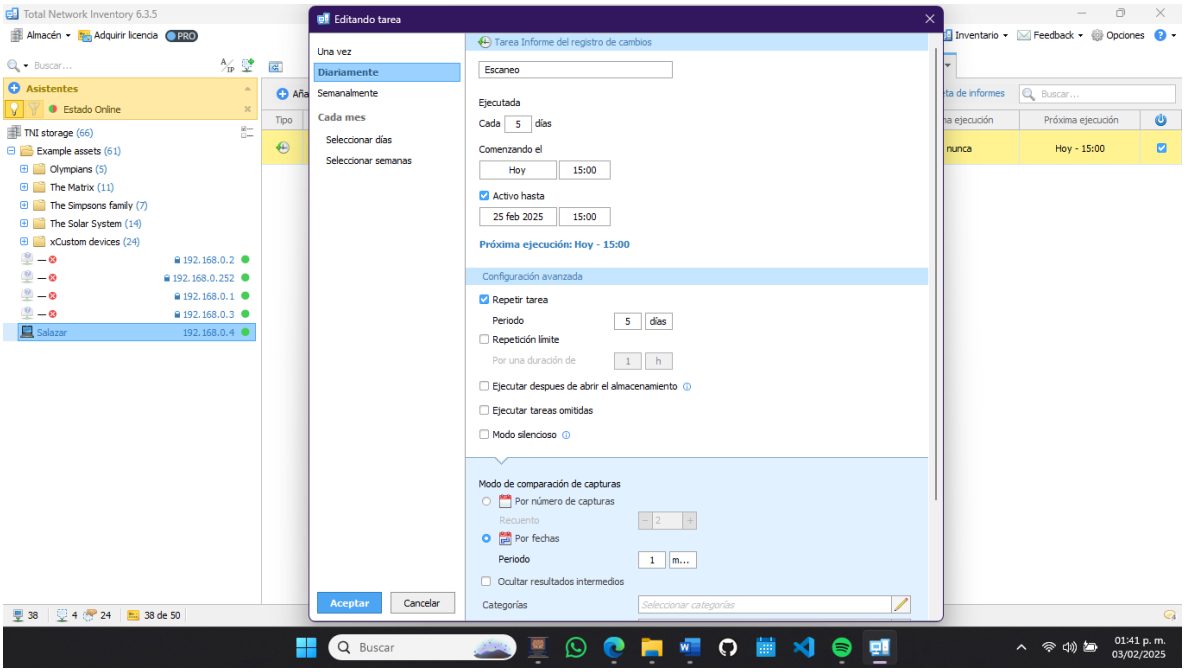


Reporte de Sistema Operativo

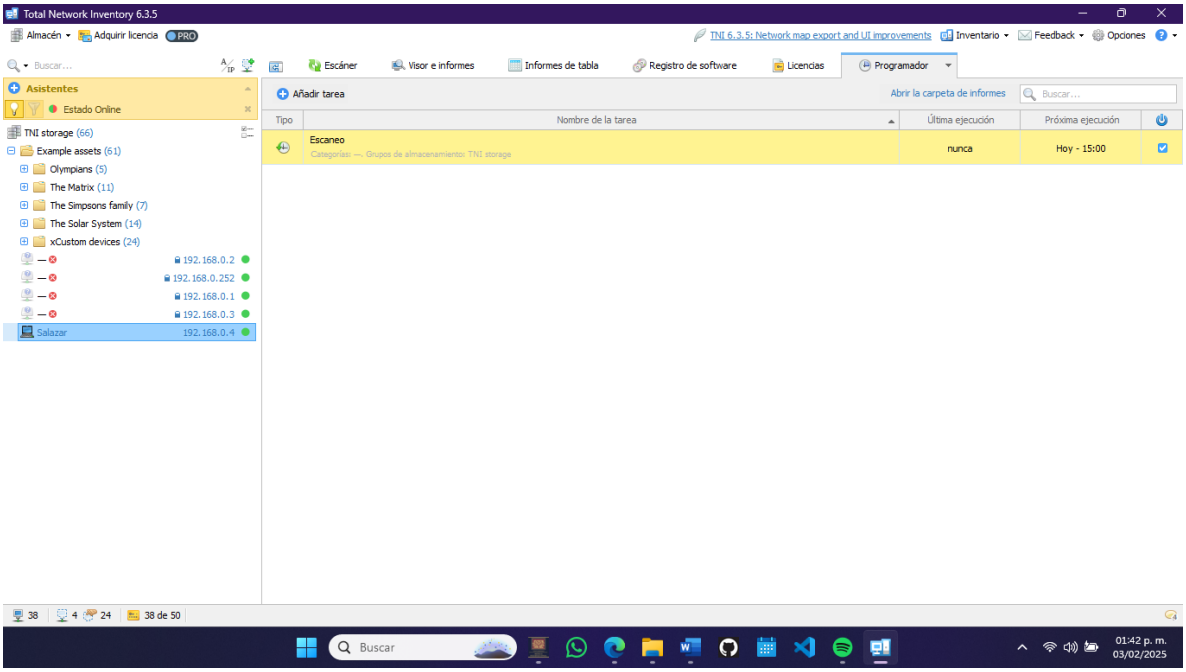


Reporte de Seguridad

Auditoria semanal y reporte



Programando escaneo



Escaneo programado

CONCLUSIÓN

La realización de la actividad de monitoreo de red destaca la importancia crítica de implementar medidas de seguridad proactivas tanto en el ámbito laboral como en la vida cotidiana. En el entorno profesional, el monitoreo constante de la red es fundamental para garantizar la integridad, confidencialidad y disponibilidad de la información, aspectos esenciales para la continuidad operativa de cualquier organización. La capacidad de identificar y analizar dispositivos conectados, detectar accesos no autorizados y evaluar vulnerabilidades en tiempo real permite anticiparse a posibles amenazas cibernéticas y actuar de manera oportuna para mitigar riesgos.

En el campo laboral, la configuración de auditorías semanales asegura un control constante sobre los recursos tecnológicos, permitiendo la identificación de cambios inusuales en el sistema, hardware, software, licencias y la red en general. Este proceso no solo facilita la detección temprana de incidentes de seguridad, sino que también contribuye al cumplimiento de normativas legales y regulatorias, fortaleciendo la postura de seguridad de la organización y protegiendo sus activos más valiosos.

En la vida cotidiana, la aplicación de estos conocimientos es igualmente relevante. El uso de redes domésticas seguras, la gestión adecuada de contraseñas, la supervisión del tráfico de red y la detección de dispositivos desconocidos pueden prevenir el robo de información personal y el acceso no autorizado a dispositivos inteligentes. Además, la práctica de mantener bitácoras de actividad y revisarlas periódicamente puede ser útil para identificar comportamientos sospechosos en entornos personales.

En conclusión, la actividad de monitoreo de red no solo fortalece las competencias técnicas en seguridad informática, sino que también fomenta una cultura de prevención y vigilancia continua. Este enfoque proactivo es esencial para proteger tanto los entornos profesionales como los personales frente a las crecientes amenazas cibernéticas en el mundo digital actual.