Actividad 2 – Monitoreo de Red

Seguridad Informática II

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Kathya Viridiana Chávez Domínguez

Fecha: 06/10/2024

Índice

Introducción

El monitoreo de red es un proceso que implica la supervisión constante y el análisis de todos los componentes de una red informática, con el objetivo de garantizar su rendimiento, disponibilidad y seguridad. Su propósito principal es anticiparse a los problemas en lugar de atenderlos solo cuando surgen, buscando prevenir en lugar de corregir.

A través de esta actividad, tendremos la oportunidad de trabajar con un software de monitoreo, Total Network Inventory, que nos permitirá escanear nuestra red e identificar los dispositivos conectados. Esto nos permitirá familiarizarnos y practicar los diferentes elementos y funcionalidades que ofrece esta herramienta de monitoreo. Al finalizar, se pretende comprender como el monitoreo de redes contribuye a la prevención de ataques cibernéticos, además de adquirir conocimientos sobre el uso de Total Network Inventory, una solución integral de gestión y auditoria de rees que proporciona un conjunto de herramientas para la administración y auditoría de PC.

Descripción

En esta ocasión se pretende utilizar algunas técnicas de protección ante ataques de explotación y acceso no autorizado a sistemas, mediante la auditoría y el monitoreo de la red. Para ello, es necesario analizar los factores que enfatizan la importancia de la seguridad y que se describen a continuación:

- Prevenir los ataques de acceso.
- Prevenir acceso a las redes.
- Validar las licencias de sus recursos por cuestiones de los aspectos legales y regulatorios.
- Control total y auditoría cada semana del sistema, hardware, software, licencias y red.
- Monitoreo completo de la red.
- Es importante que se guarde la bitácora, eliminarla e iniciar una nueva para ddetectar los cambios desde el día 1.

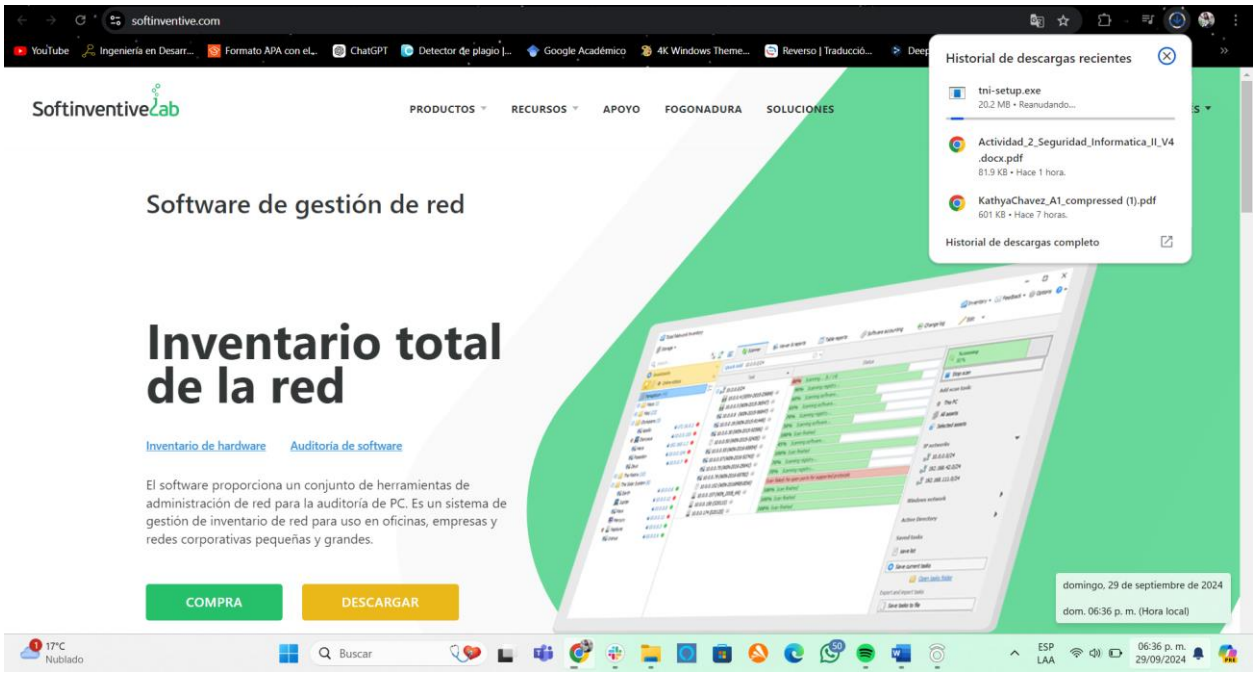
Para llevar a cabo la actividad, será necesario instalar un software de monitoreo que permita escanear la red e identificar los dispositivos conectados en ella. Una vez que tengamos este análisis debemos generar un reporte detallado que identifique cada aspecto relevante y configurar una auditoría semanal utilizando la opción “Programación de auditoría”.

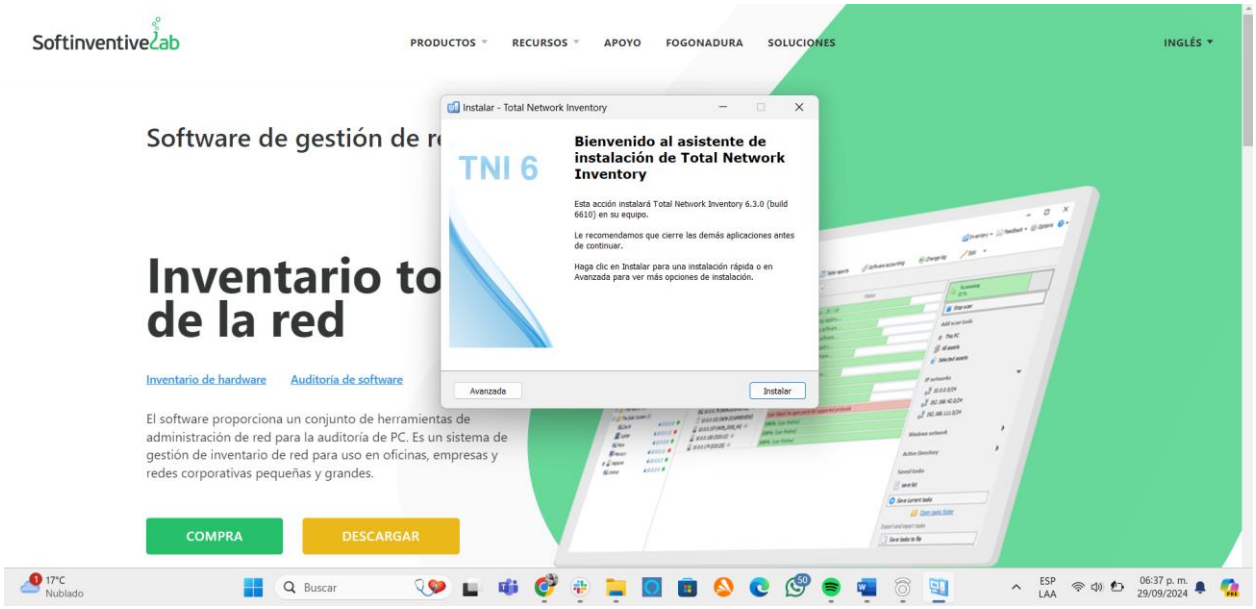
Justificación

En la actualidad, vivimos en un mundo altamente interconectado y digital, por lo que el monitoreo de red se ha convertido en una parte esencial tanto en la gestión de sistemas como en la seguridad cibernética de las organizaciones. Implementar este monitoreo en las organizaciones ofrece diferentes ventajas, como la detección temprana de problemas antes de que afecten a los usuarios finales, incluyendo fallos en dispositivos, congestión de la red y amenazas en la seguridad. Además, contribuye a mejorar la protección ayudando a identificar actividades sospechosas, como intrusiones o la presencia de malware, permitiendo tomar medidas preventivas para proteger la red y los datos sensibles. Por estas y otras razones, el monitoreo de redes es una práctica fundamental para cualquier organización que dependa de las comunicaciones en red. A medida que la tecnología avanza, el monitoreo de redes se vuelve indispensable para garantizar la integridad de cualquier infraestructura de TI.

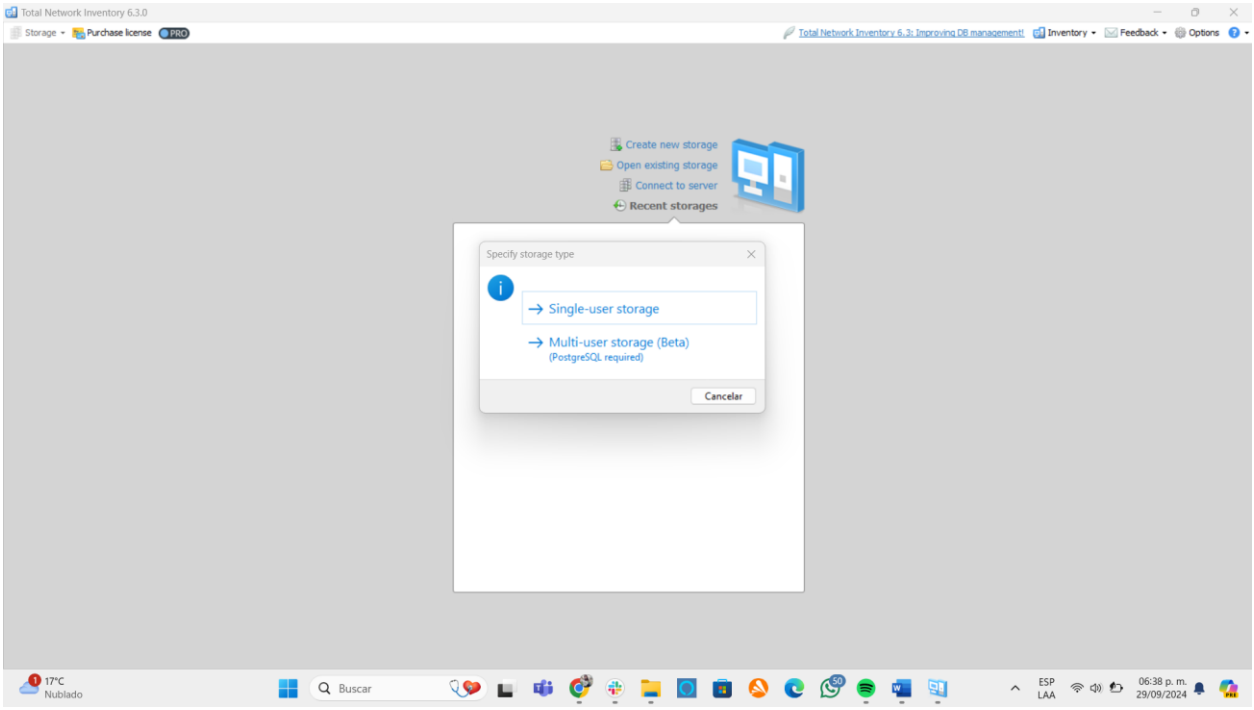
Desarrollo

Para esta actividad, comenzaremos descargando la herramienta de software Total Network Inventory (TNI). Esta herramienta nos permitirá recopilar y analizar la información detallada sobre nuestro equipo, además de generar informes completos y exportables sobre su estado, l que facilita la gestión de inventarios y auditorias de TI.

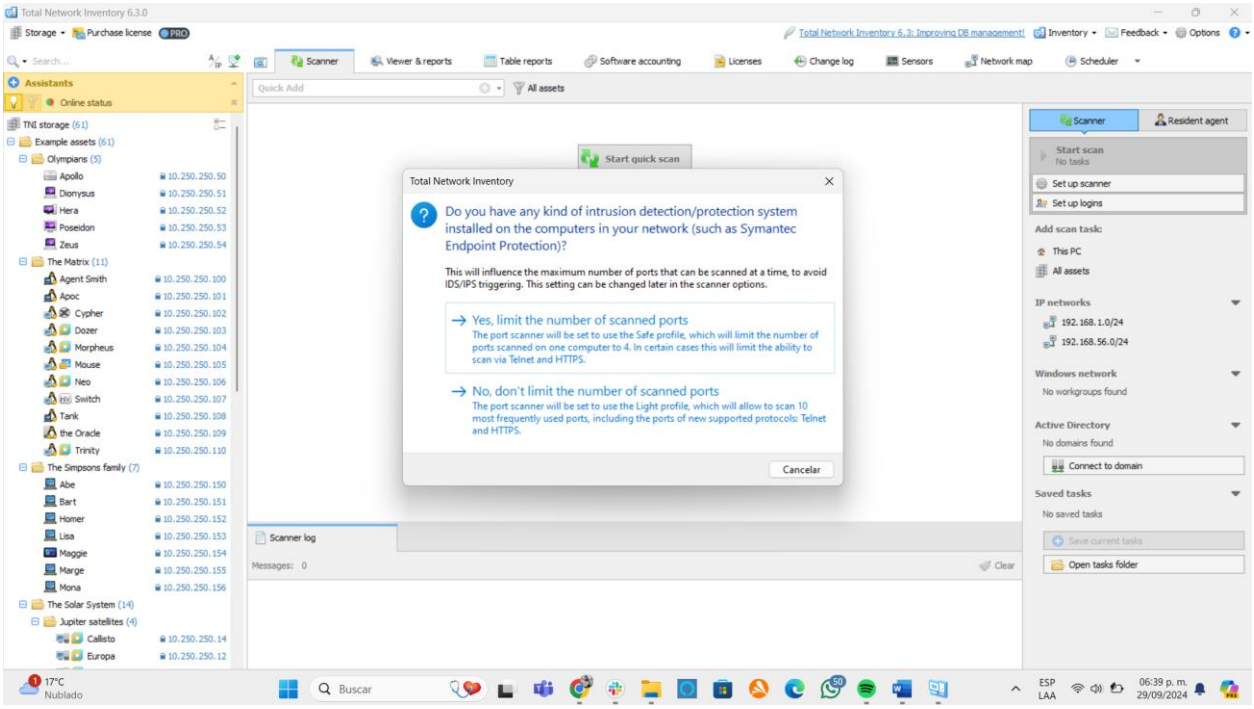




Como podemos observar, la instalación de TNI es un proceso muy sencillo. Una vez dentro de la herramienta, se nos solicita seleccionar el tipo de almacenamiento que se utilizará para guardar los datos del inventario, eligiendo entre el almacenamiento de un solo usuario o de múltiples usuarios. Para esta actividad, seleccionaremos la opción del almacenamiento de un solo usuario.

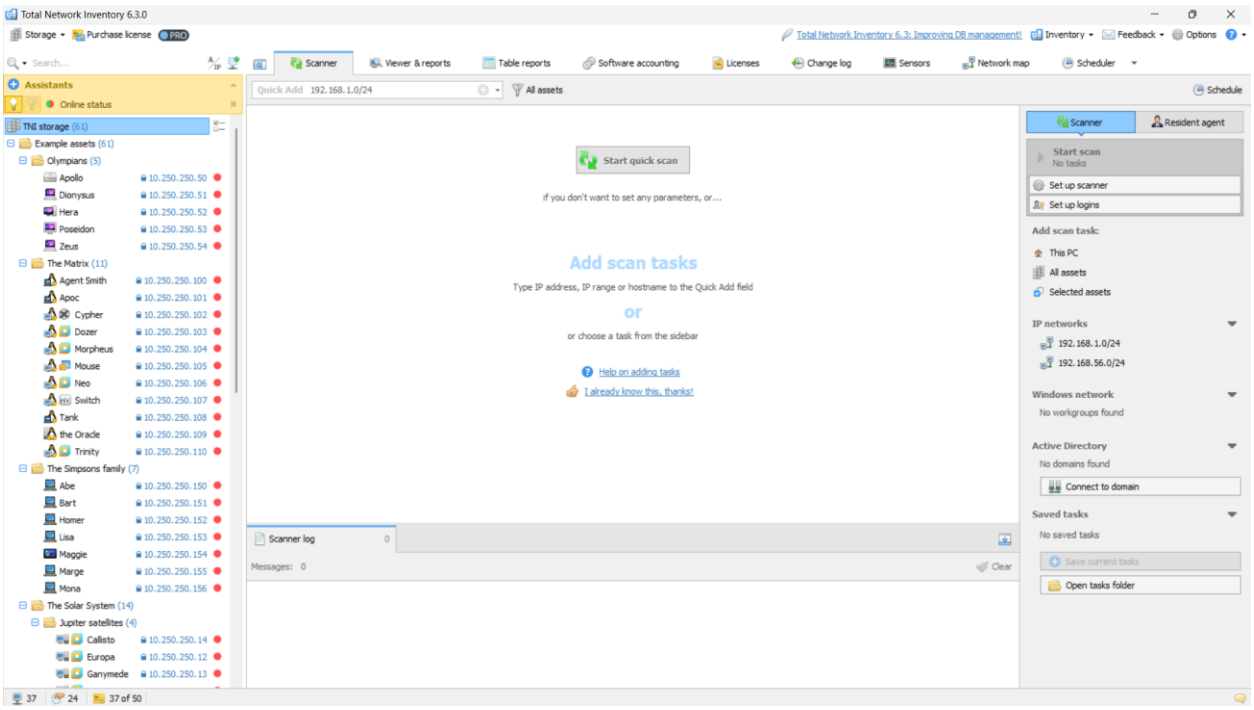


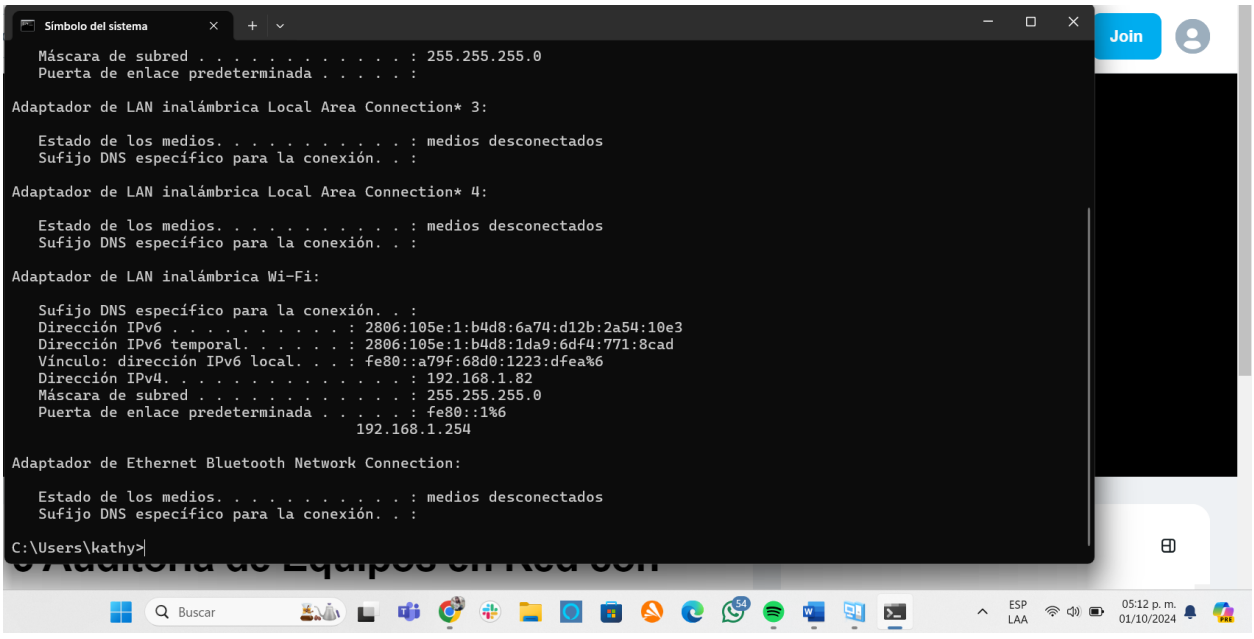
Para la configuración del escaneo de puertos, se nos pide seleccionar una opción que permite identificar si la red cuenta con un sistema de detección o protección de intrusiones, con el fin de evitar que estos sistemas clasifiquen la actividad del escaneo como una actividad maliciosa. Se nos da dos opciones; Si, limitar el número de puertos escaneados y No, no limitar el número de puertos escaneados. La opción a seleccionar dependerá de la configuración de seguridad de nuestra red y de la profundidad del escaneo que queramos realizar. En esta practica, utilizaremos la opción de no limitar el número de puertos escaneados, esto con la finalidad de obtener un escaneo más amplio.



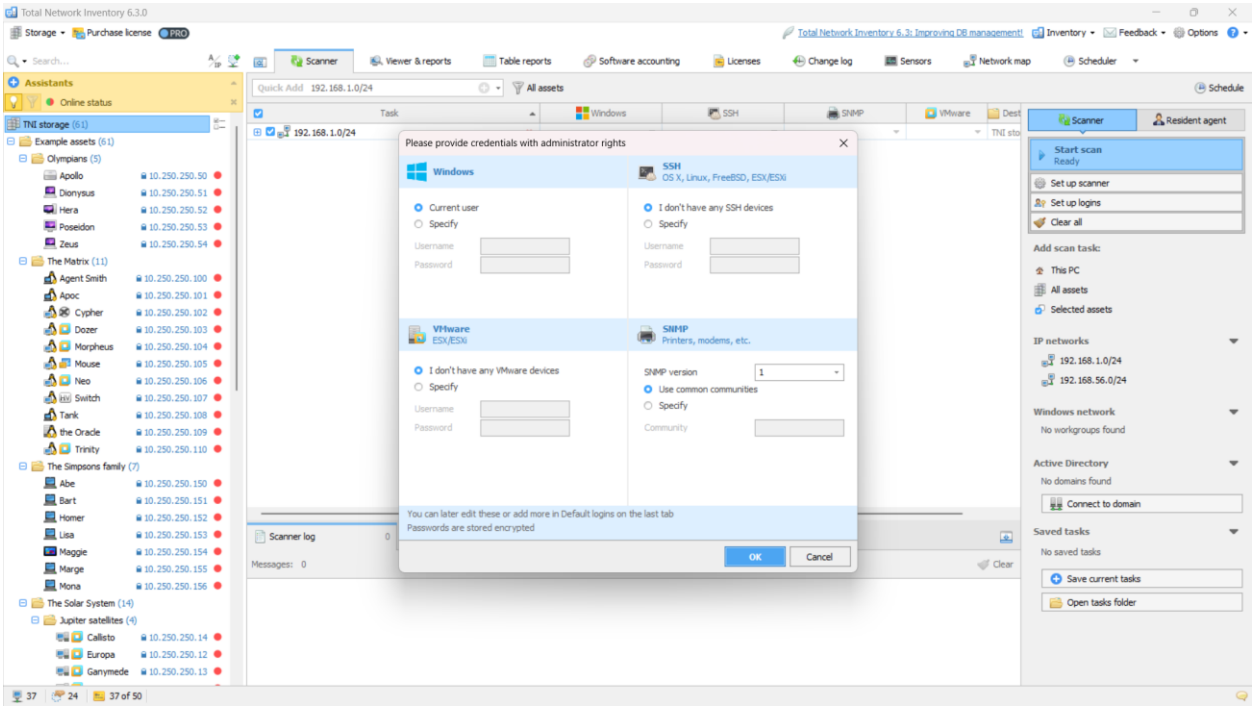
Resultado del escaneo

Para iniciar el escaneo, primero debemos verificar nuestra dirección IP y su rango. Esto se puede hacer desde la línea de comandos (cmd) utilizando el comando ipconfig.

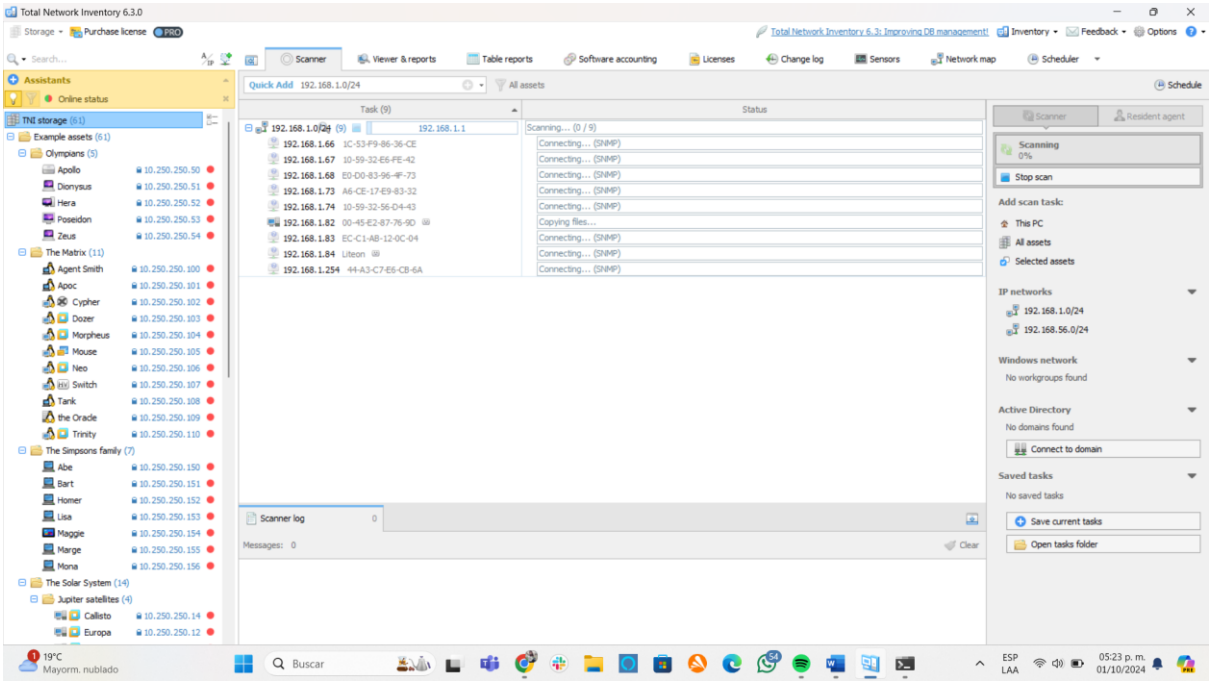


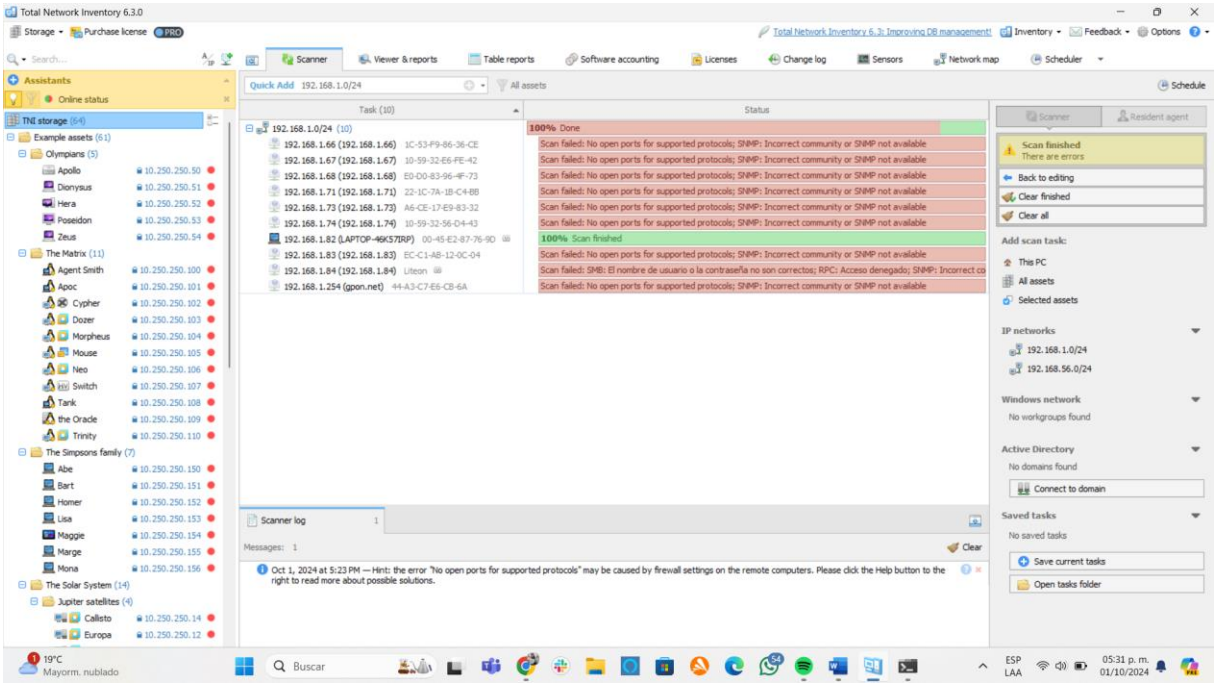


Una vez confirmada la dirección IP, se mostrará una ventana que solicita credenciales de administrador para realizar el escaneo de la red. Como podemos observar, se nos dan diferentes opciones que corresponden a diferentes tipos de dispositivos o métodos de autenticación que TNI puede utilizar para acceder a los activos en la red. La opción a seleccionar dependerá de los dispositivos que se deseen escanear. Si la red contiene varios tipos de dispositivos, podemos marcar las opciones correspondientes para cada uno y proporcionar las credenciales necesarias. En nuestro caso seleccionaremos las credenciales de Windows.



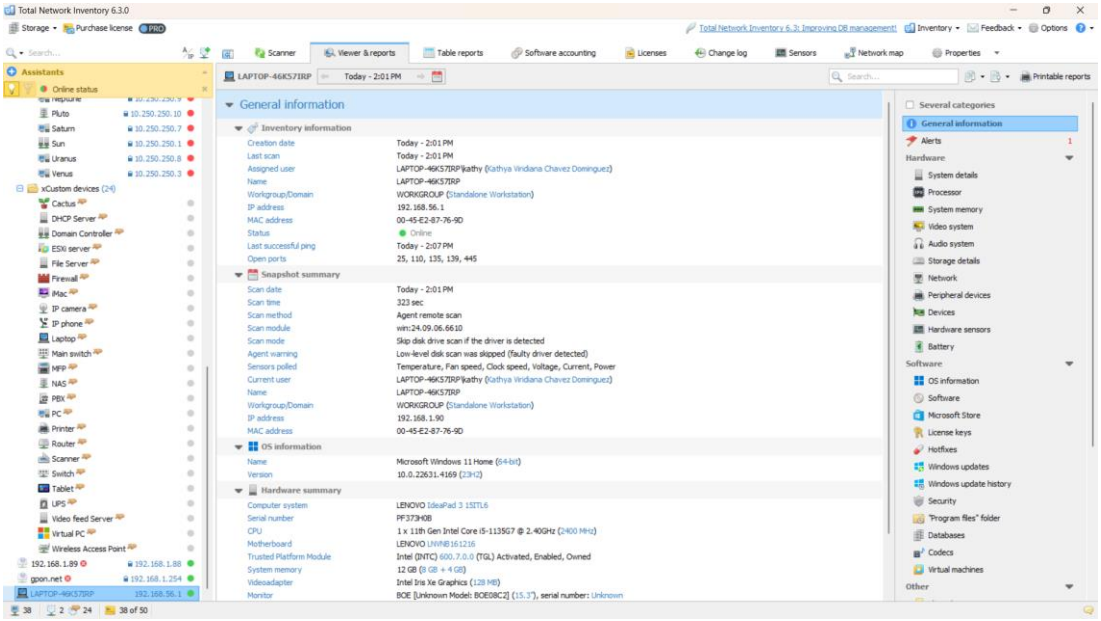
De esta forma, comenzará el escaneo de los dispositivos seleccionados, en nuestro caso, el dispositivo con la IP 192.168.1.82 (Laptop-46K57IRP). Una vez finalizado el escaneo, en esta misma pantalla veremos que el progreso ha alcanzado el 100%.

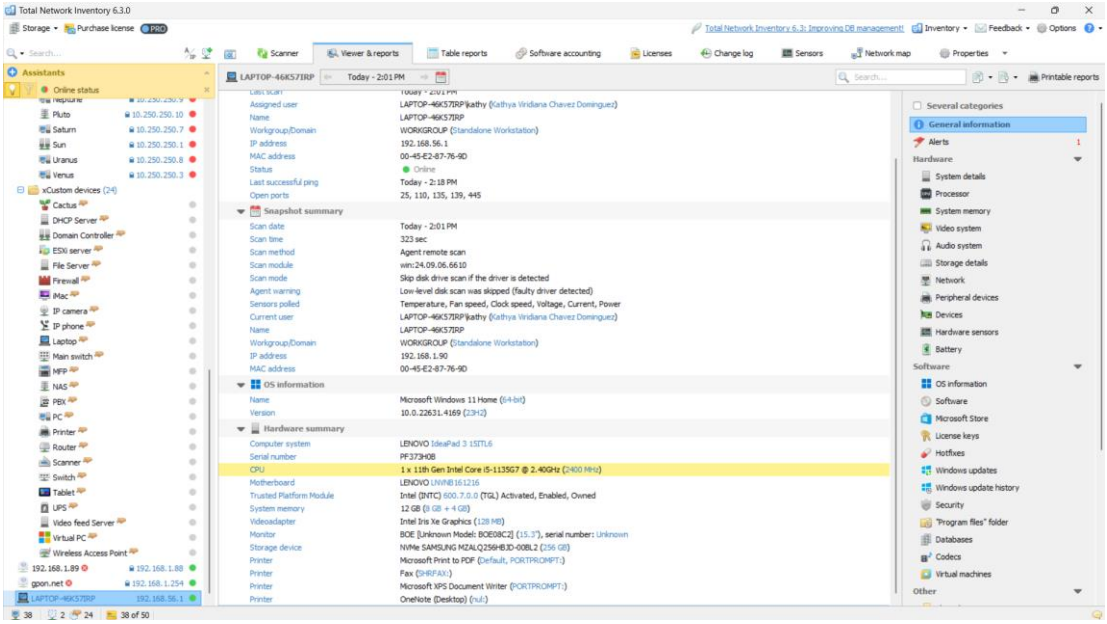




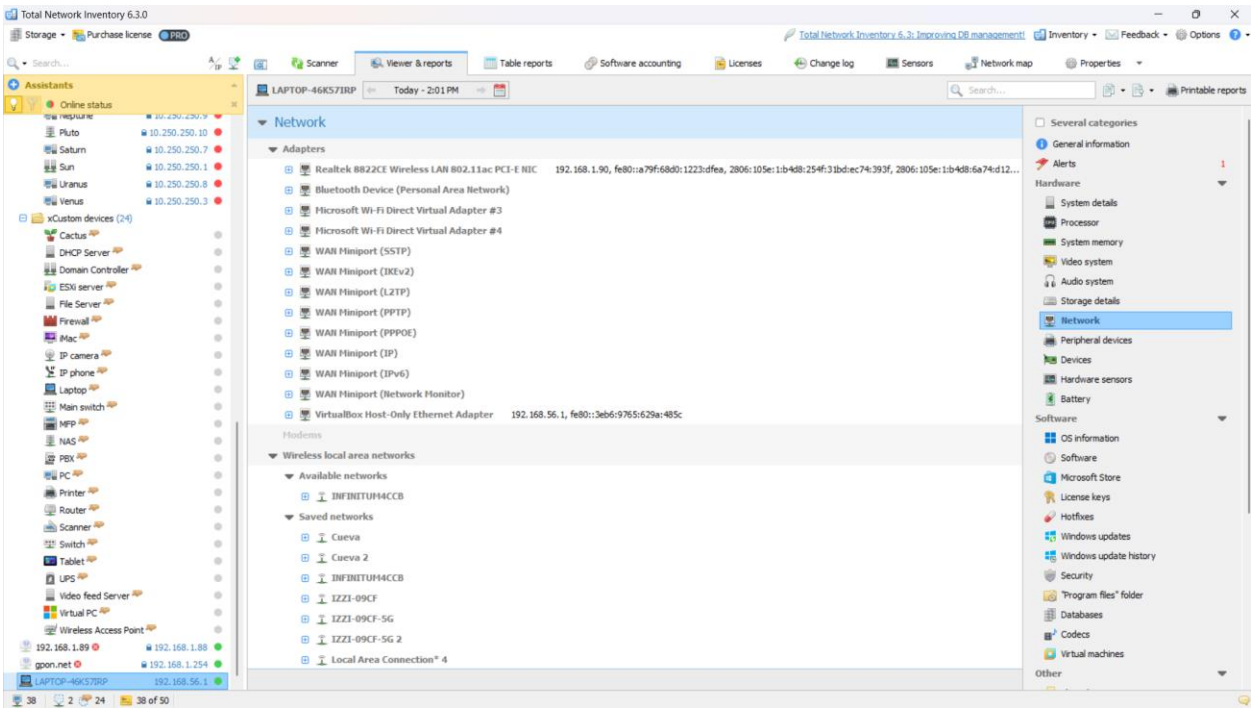
Reporte

Una vez finalizado el escaneo, podemos acceder al apartado de Visor e Informes, el cual nos ofrece una vista detallada de los datos recolectados durante el análisis de la red. Además, si es necesario, permite generar informes personalizados. De esta manera podemos gestionar, analizar y documentar el estado de la red de forma eficiente.

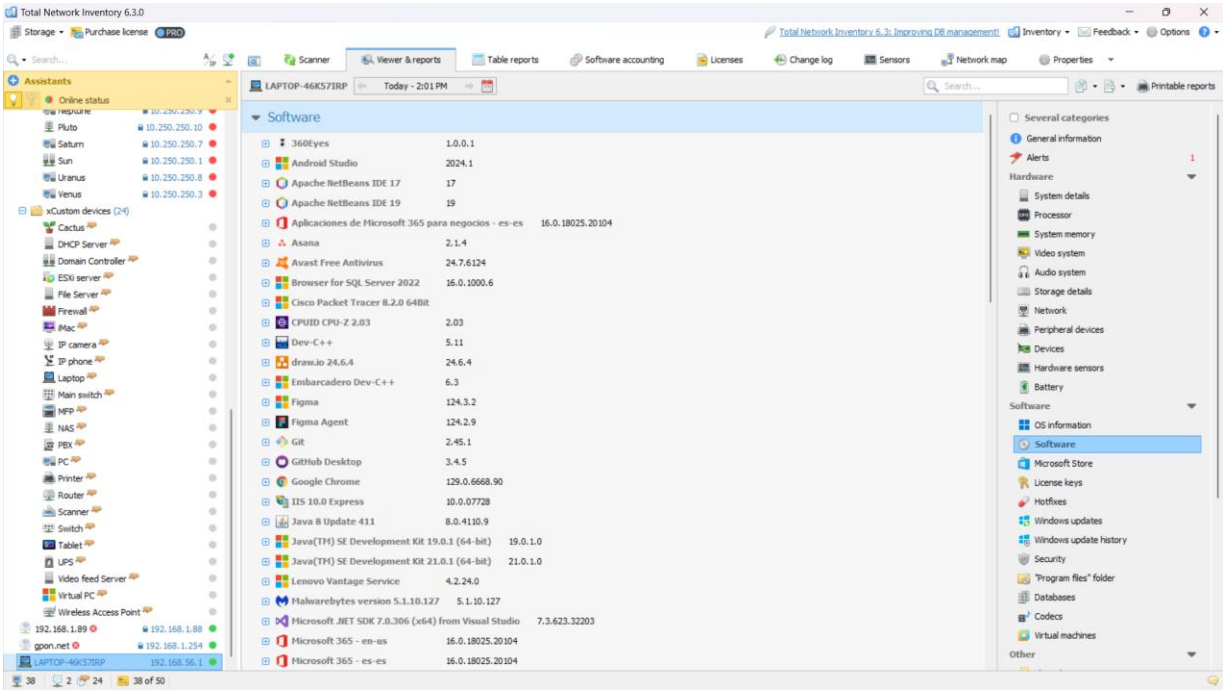


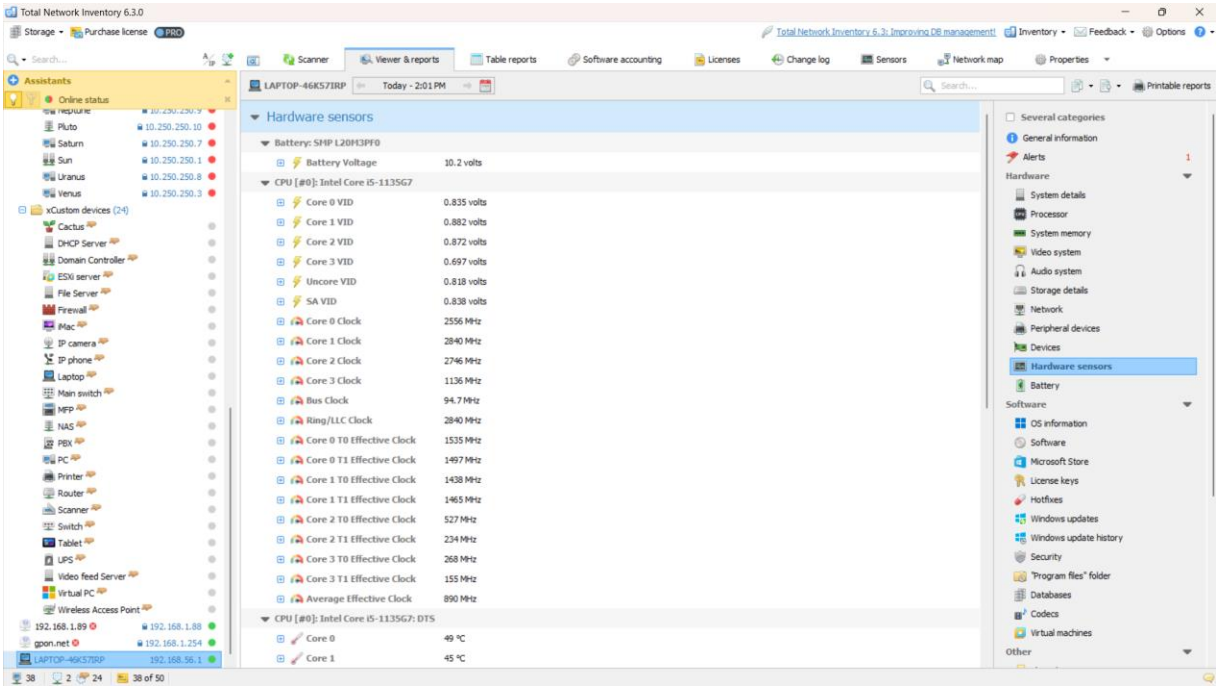


En este reporte podemos ver la información relacionada con los adaptadores de red disponibles en el dispositivo, las direcciones IP asignadas y las redes a las que el equipo puede acceder o se ha conectado previamente.



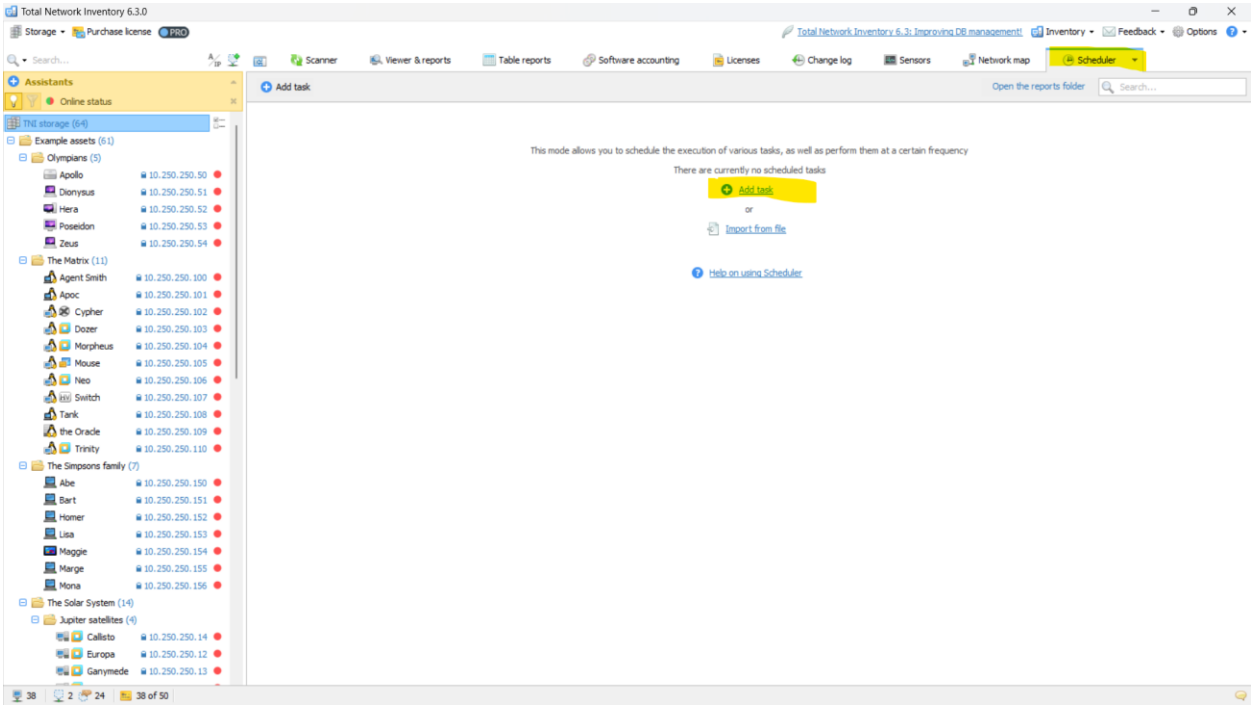
Como podemos observar, TNI ofrece una variedad de reportes que proporcionan información detallada sobre el software, hardware, y otros datos relevantes para el análisis y funcionamiento del dispositivo. Estos reportes, permiten obtener una visión completa de los activos, facilitando la gestión y el monitoreo del estado de cada equipo.



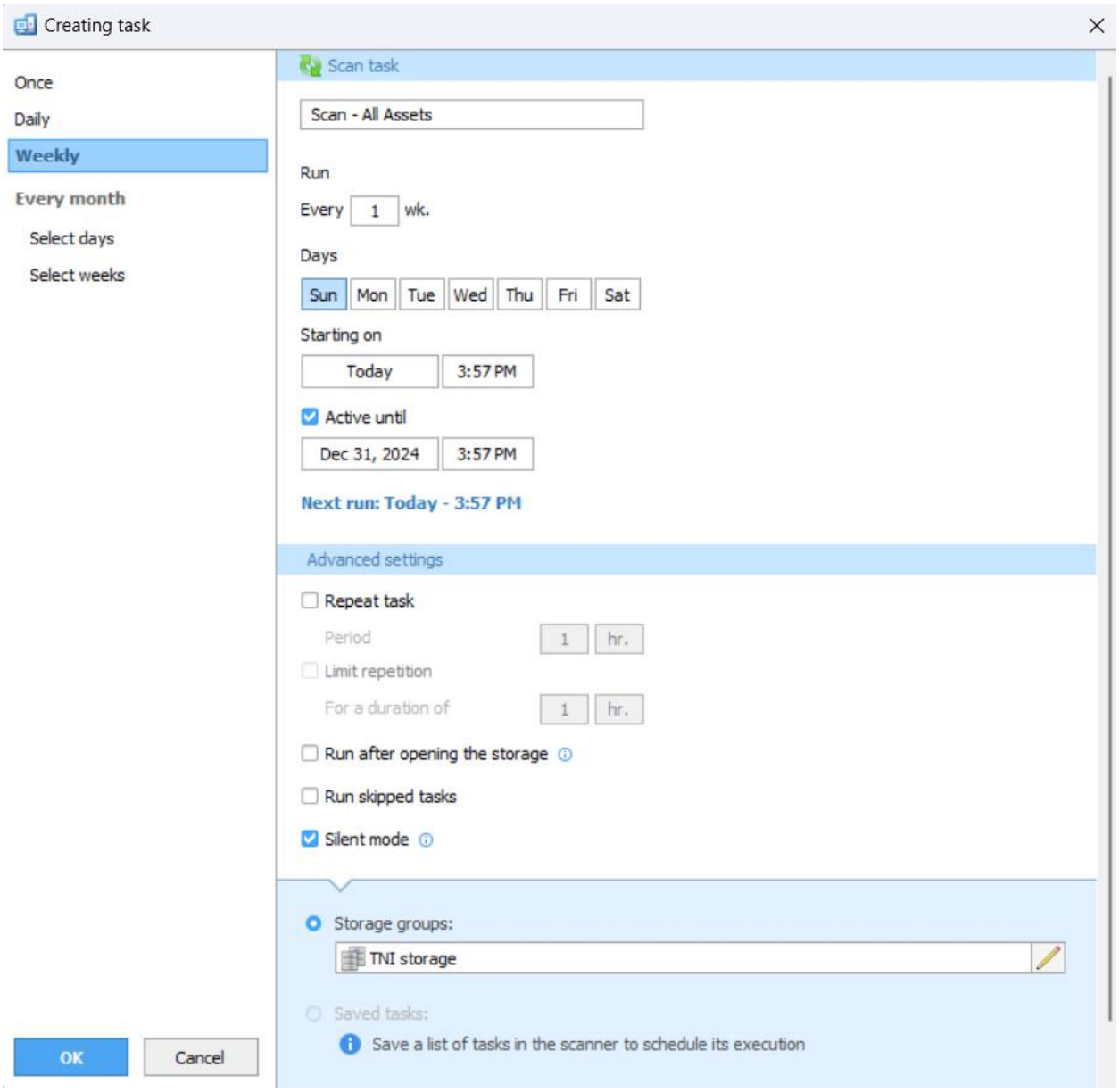


Auditoria semanal y reporte

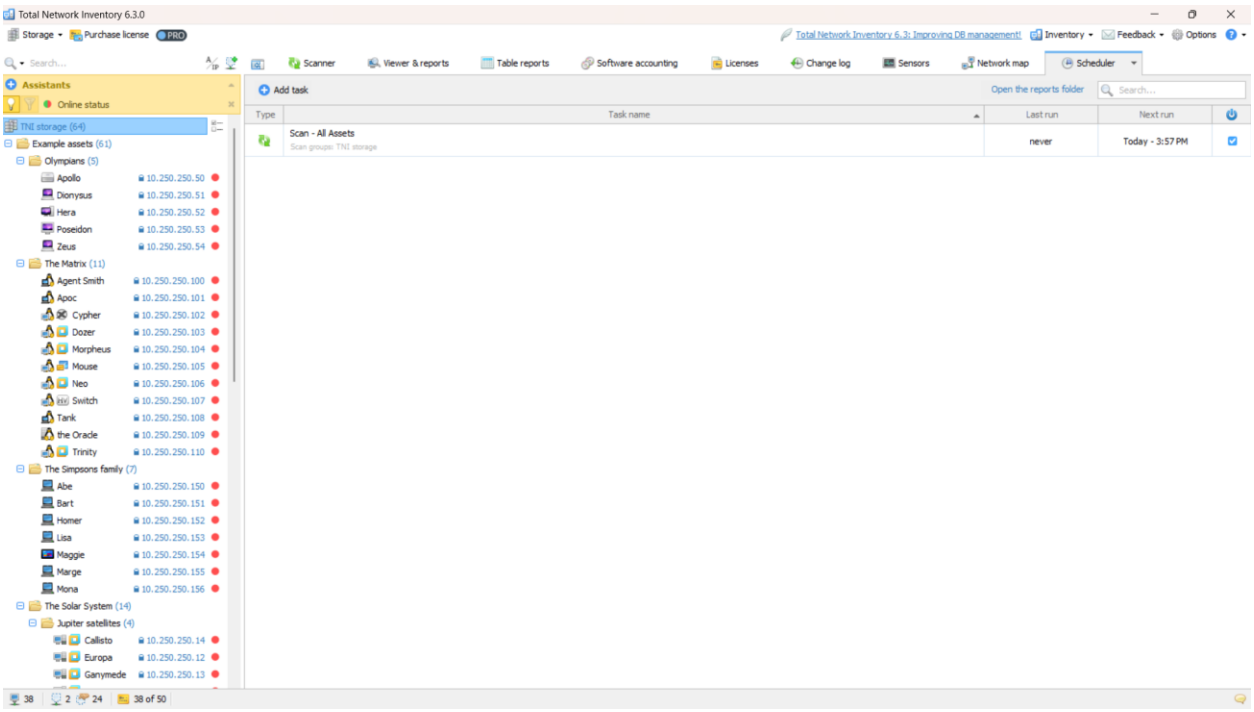
Para configurar una auditoria semana en TNI, debemos utilizar la opción de Programación de auditoría, que se encuentra en la parte superior derecha. Al seleccionarla, se abrirá una ventana donde podemos programar las auditorias de manera automática. Una vez que estamos en esta ventana debemos hacer clic en Agregar tarea o Add Task para comenzar la configuración.



En este ventana, debemos seleccionar la opción semanal o weekly, que indica la periodicidad con la que se realizará la auditoria. También es necesario elegir el día de la semana y la hora exacta en que queremos que la auditoría se ejecute. Una vez configurados los parámetros de la tarea debemos guardar la información.



De esta manera la auditoria programada se ejecutará cada semana en la fecha y hora configuradas. Cabe mencionar que los resultados pueden ser visualizados en el apartado de Visor e Informes o bien, recibir notificaciones si la tarea fue completada exitosamente.



.

Conclusión

A través de esta actividad, tuvimos la oportunidad de trabajar con Total Network Inventory, una herramientas de software diseñada para la gestión y monitoreo de redes. Esto nos permitió practicar y explorar sus diferentes funcionalidades para el escaneo y la recopilación de información detallada sobre la red y los dispositivos conectados a ella.

Los reportes que analizamos nos proporcionaron información relevante sobre nuestro equipo, lo que resalta la facilidad con la que las organizaciones pueden monitorear y proteger los diferentes dispositivos que se conectan a su red, para así poder asegurar su correcto uso y reducir riesgos de intrusiones o vulnerabilidades. Además. pudimos realizar la programación de auditorías periódicas para mantener un registro actualizado de los activos de la red, lo que ayuda a detectar cambios o problemas de seguridad. Gracias a esta actividad, comprendemos la importancia de realizar escaneos y auditorias periódicas para la gestión de redes, lo que permite a los administradores supervisar, auditar y optimizar el rendimiento de los activos de TI en su organización.

Link GitHub: https://github.com/KathyaCh/Monitoreo-de-red.git

Referencias

I. *Acerca de total network inventory*. (s. f.). ComponentSource. https://www.componentsource.com/es/product/total-network-inventory/about

II. Arguelles, G. T. (2023, 12 noviembre). El monitoreo de red: garantizando la estabilidad y el rendimiento. *Access Quality - Presentación digital*. https://www.accessq.com.mx/monitoreo-de-red/

III. Diego Macias. (2020, 9 diciembre). *Total Network Inventory-Herramienta de auditoria para PC* [Vídeo]. YouTube. https://www.youtube.com/watch?v=WRuOv-vIDew

IV. ManageEngine. (s. f.). *Conceptos básicos de monitoreo de red | ¿Qué es monitoreo de red? - ManageEngine OpManager*. https://www.manageengine.com/latam/network-monitoring/monitoreo-de-red-conceptos-basicos.html

V. *¿Qué es el monitoreo de red? | IBM*. (s. f.). https://www.ibm.com/mx-es/topics/network-monitoring

VI. Seguridad, P. (2022, 14 septiembre). *La importancia de monitorear una red de datos en una organización*. Protek. https://www.protek.com.py/novedades/monitorear-una-red-de-datos/

VII. Softinventive Lab. (s. f.). *Network management software: network inventory, server monitoring, software deployment | Softinventive.com*. https://www.softinventive.com/

VIII. Softinventive Lab. (2021b, noviembre 22). *Total Network Inventory 6: solución de inventario de software y auditoría de PC.* [Vídeo]. YouTube. https://www.youtube.com/watch?v=rBbPf_fa3h4