

Proyecto Final - Auditoria y Bitácora

Seguridad Informática 2

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Fernando Pedraza Garate

Fecha: 30 de mayo 2024

Índice

Etapa 1 – Detección y prevención de ataques de acceso

- Introducción. Pág. 4 - 6
- Descripción Pág. 7 - 8
- Justificación Pág. 9 - 10
- Desarrollo Pág. 11 - 22
 - Incidencias encontradas
 - Reporte
 - Análisis de identificación de mejoras

Etapa 2 – Monitoreo de red

- Desarrollo Pág. 23 - 34
 - Resultado del escaneo
 - Reporte
 - Auditoria semanal y reporte

Etapa 3 – Auditoria y Bitácora

- Desarrollo Pág. 35 - 42
 - Auditoria y bitácora
 - Auditoria de equipo
 - Bitácora
 - Importancia de seguridad (Prevención, Monitoreo, Auditoria)
- Conclusión Pág. 43 - 44
- Referencias Pág. 45

Introducción

La detección y prevención de ataques de acceso son componentes esenciales en la seguridad informática y de la información, donde la detección de ataques de acceso hace referencia a la identificación de intentos no autorizados por acceder a sistemas, redes o datos, todo esto mediante herramientas y técnicas que monitorean y analizan el tráfico de la red y las actividades en los sistemas para identificar comportamientos sospechosos o anómalos que puedan indicar un ataque, mientras que la prevención de ataques de acceso consta en la implementación de medidas y controles que impidan que los ataques de acceso no autorizado tengan éxito, utilizando como herramientas firewalls, sistemas de prevención de intrusiones (IPS), sistemas de detección de intrusos (IDS), autenticación multifactor (MFA), políticas de contraseñas robustas, y otras medidas de seguridad.

La protección de datos sensibles como la información confidencial, datos personales, financieros y propiedad intelectual, deben estar protegidos contra accesos no autorizados para evitar la exposición y el robo de los mismos manteniendo **la integridad del sistema** para asegurar que los sistemas permanezcan íntegros y operacionales, evitando que se puedan alterar, corromper o destruir datos y sistemas.

El monitoreo de red implica la supervisión constante de una red informática para detectar problemas de rendimiento, fallos de hardware, brechas de seguridad y otros inconvenientes que pueden afectar la operatividad y eficiencia de la misma, este proceso incluye la recolección de datos en tiempo real y el análisis de estos para identificar patrones y anomalías.

Los componentes del monitoreo de red implican la recopilación de datos por medio de herramientas de software y hardware para recolectar información sobre el tráfico de red, el estado de los dispositivos conectados como los Routers, Switches, Servidores y Estaciones de trabajo, y el rendimiento de aplicaciones y servicios, donde los datos recopilados se analizan para detectar tendencias, identificar problemas potenciales y evaluar el rendimiento de la red, con los sistemas de monitoreo se generan alertas automáticas que detectan problemas como caídas de red, picos de tráfico inusuales o fallos en dispositivos críticos, proporcionando informes y paneles de control visuales que resumen el estado de la red, ayudando a los administradores a entender la salud y el rendimiento de la infraestructura

Existen diversas herramientas que facilitan este trabajo, una de las más conocidas que ofrece monitoreo de red y de sistemas es Nagios, para el monitoreo de código abierto en tiempo real, esta Zabbix, como solución comercial para el monitoreo y gestión de red, esta Solar Winds Network Performance Monitor (NPM), y la que ofrece una amplia gama de sensores para diferentes tipos de monitoreo, esta PRTG Network Monitor.

Dentro de la seguridad informática las bitácoras y auditorias son componentes fundamentales para la identificación de vulnerabilidades que pueden ser explotadas, permitiendo identificar y evaluar riesgos en los sistemas y redes informáticas, previniendo brechas de seguridad de forma anticipada, ayudando a las industrias en el cumplimiento normativo para evitar sanciones y así mantener la confianza de sus clientes, ya que muchas de estas están sujetas a regulaciones que exigen auditorias regulares para poder obtener o mantener su certificación de seguridad ISO, proporcionando información valiosa para la optimización y mejorar sus políticas, procedimientos, y controles de seguridad, identificando las áreas donde se necesita capacitación adicional para concienciación del personal y en caso de algún incidente de seguridad proporcionen un registro detallado que puede ser usado en el análisis forense para determinar el origen y el alcance del incidente, revisando la efectividad de los controles existentes y hacer los ajustes necesarios para prevenir futuras incidencias.

Las bitácoras permiten el monitoreo y detección de las actividades sospechosas registrándolas en los sistemas, para posteriormente proporcionar un rastro detallado de lo que ha ocurrido, detectando comportamientos anómalos o actividades sospechosas que pueden indicar intentos de intrusión o violaciones de seguridad que permitan investigar y entender los incidentes presentados, manteniendo una evidencia para análisis forense y así tomar las acciones correctivas pertinentes, manteniéndolas por un tiempo determinado para demostrar el cumplimiento normativo siguiendo los procedimientos adecuados para una mejora continua. (*ChatGPT*, n.d.)

Definición del contexto.

Para esta actividad se utilizarán algunas técnicas de protección ante ataques de explotación y obtención de acceso a los sistemas que permitan realizar auditorías a la red mediante herramientas tecnológicas, ya sea especializadas o que presenten la funcionalidad de auditoría, como un sistema de detección de intrusos (IDS), un sistema de prevención de intrusos (IPS), autenticación multifactor (MFA), o firewalls.

En este sentido, se requiere se analicen los factores que enfatizan la importancia de la seguridad como: el monitoreo completo de la red, la prevención de ataques de acceso, y prevención de acceso a las redes, validar las licencias de los recursos por cuestiones de los aspectos legales y regulatorios, instalando y utilizando un software que permita detectar y prevenir ataques de acceso al sistema y de red, contando con un control total y auditoria semanal del sistema, hardware, software, licencias y red que valide sus vulnerabilidades ante un posible ataque de virus, a accesos no permitidos o percances en la red, monitoreándola de forma completa, y así poder generar un reporte desde la herramienta a utilizar que demuestre el resultado detallado del análisis generado.

Es importante guardar una bitácora, eliminarla e iniciar una nueva para detectar los cambios desde el primer día.

Se realizará una auditoría desde el equipo de cómputo o utilizando una herramienta especializada para identificar las licencias de los recursos instalados obteniendo información precisa de los recursos del equipo de cómputo, que de igual manera otorgue información legal respecto a las licencias obtenidas y faltantes, manteniendo un control total del equipo apertura mayor seguridad en los mecanismos que se implementen para salvaguardar los recursos valiosos como la información.

Justificación.

Muchas empresas están reguladas por leyes y normas que exigen la protección de la información y la privacidad, por lo que la detección y prevención de ataques es esencial para **cumplir con la normatividad** de estas regulaciones y así evitar sanciones legales, **previniendo pérdidas financieras** significativas debido a fraudes, robos de información, demandas legales y pérdida de la confianza por parte de los clientes, causados por algún ataque cibernético. Un incidente de seguridad puede dañar gravemente la **reputación** de una organización, suficiente razón por lo que la seguridad de la información es crucial para mantener la **confianza de los clientes y socios, así como la imagen de la empresa**, el detectar ataques en tiempo real permite una **respuesta rápida y eficiente** para poder mitigar daños, ayudando a las organizaciones a reaccionar antes de que un ataque cause un daño significativo.

Las herramientas y técnicas que pueden ayudar a cumplir con esta ardua labor son los Sistemas de Detección de Intrusos (IDS) que ayudan a monitorear y analizar el tráfico de red identificando actividades sospechosas, los Sistemas de Prevención de Intrusos (IPS) además de detectar ayudan a prevenir ataques bloqueando el tráfico malicioso, la Autenticación Multifactor (MFA) añade capas adicionales de verificación para garantizar que solo usuarios autorizados puedan acceder al sistema, los Firewalls controlan el tráfico de red entrante y saliente basándose en políticas de seguridad predefinidas y el análisis de comportamiento del usuario ayuda a identificar patrones de comportamiento inusuales que podrían indicar un acceso no autorizado.

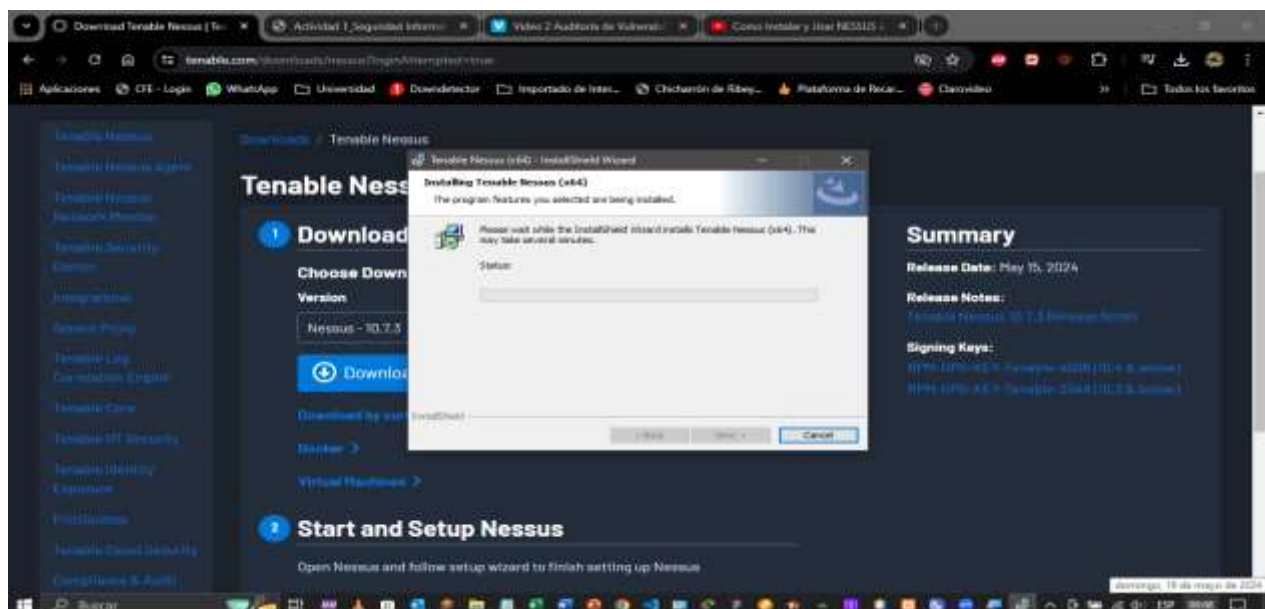
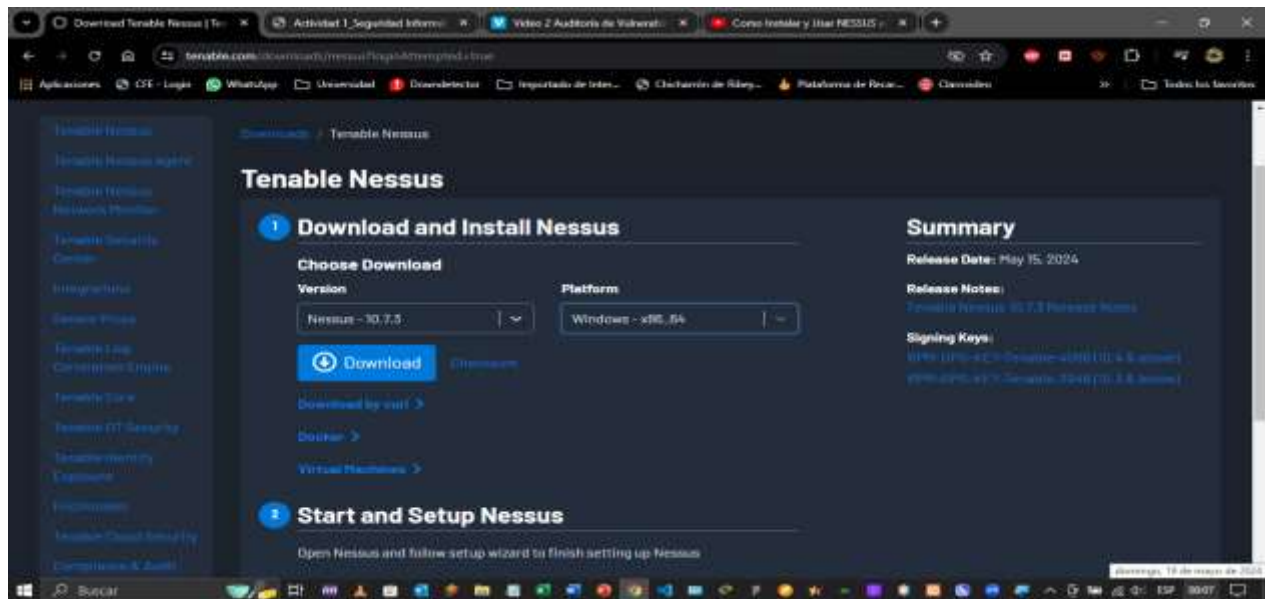
Es importante el monitoreo de red para una detección temprana de problemas, permitiendo identificarlos y solucionarlos antes de que afecten gravemente las operaciones empresariales, minimizando el tiempo de inactividad, mejorando el rendimiento al optimizar en identificar cuellos de botella y las áreas que requieran mejoras, ayudando a prevenir ataques y brechas de seguridad al detectar actividades sospechosas o no autorizadas, facilitando de forma eficiente su gestión planificando de forma adecuada las capacidades y la implementación de actualizaciones necesarias, ayudando a las organizaciones a cumplir con las regulaciones y estándares de la industria con registros detallados de la actividad de la red, reduciendo los costos asociados con tiempos de inactividad y reparaciones emergentes. (*ChatGPT*, n.d.)

Desarrollo.

Etapa 1 – Detección y Prevención de ataques de acceso

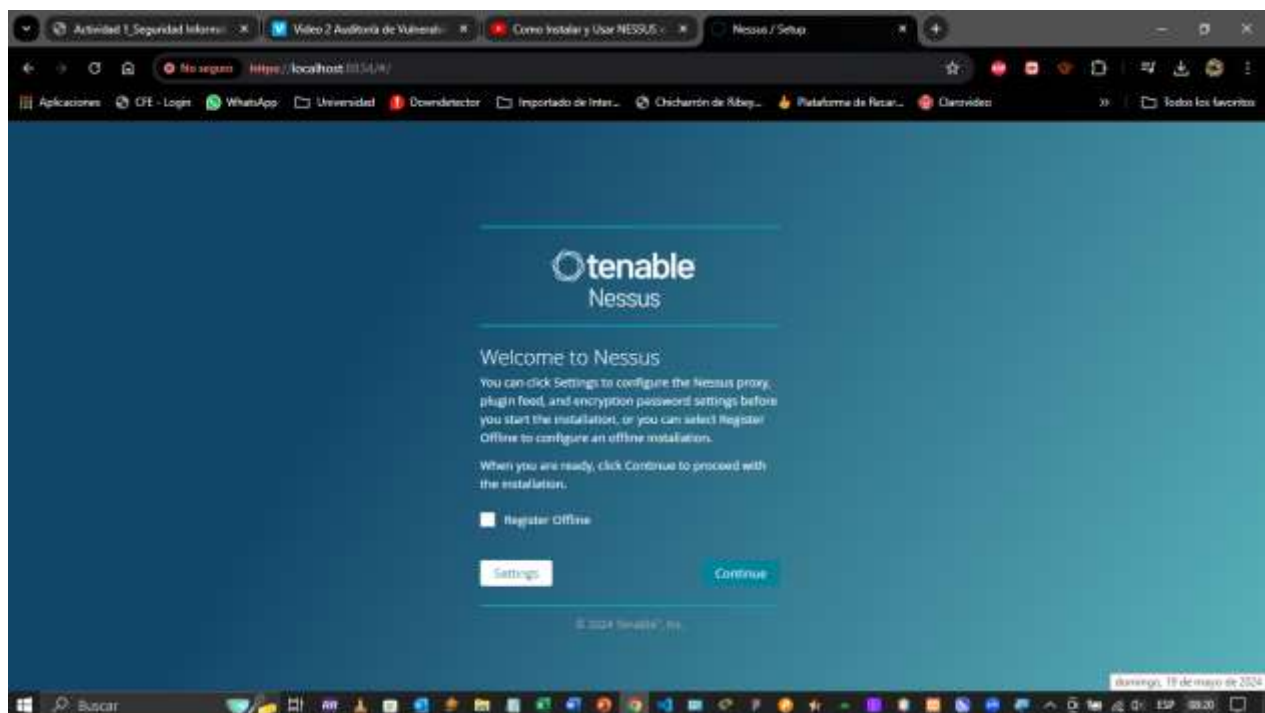
Se descarga e instala el programa a utilizar desde el siguiente enlace:

<https://www.tenable.com/downloads/nessus?loginAttempted=true>

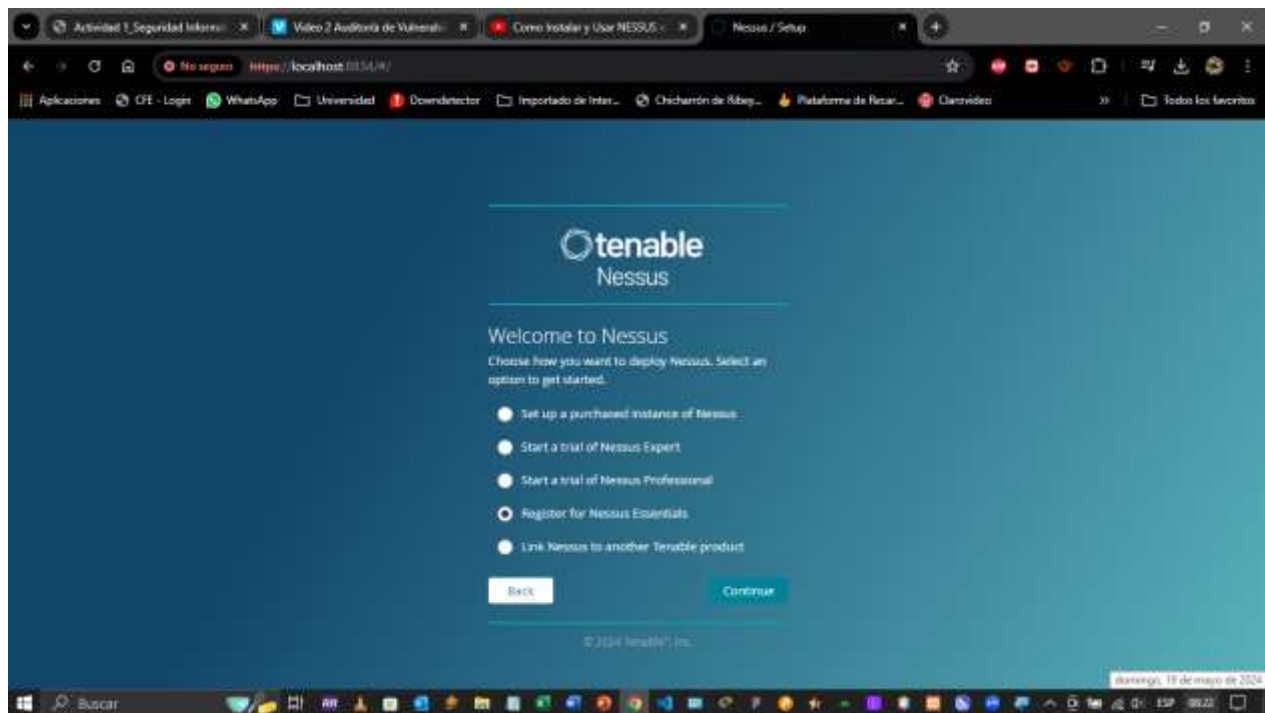




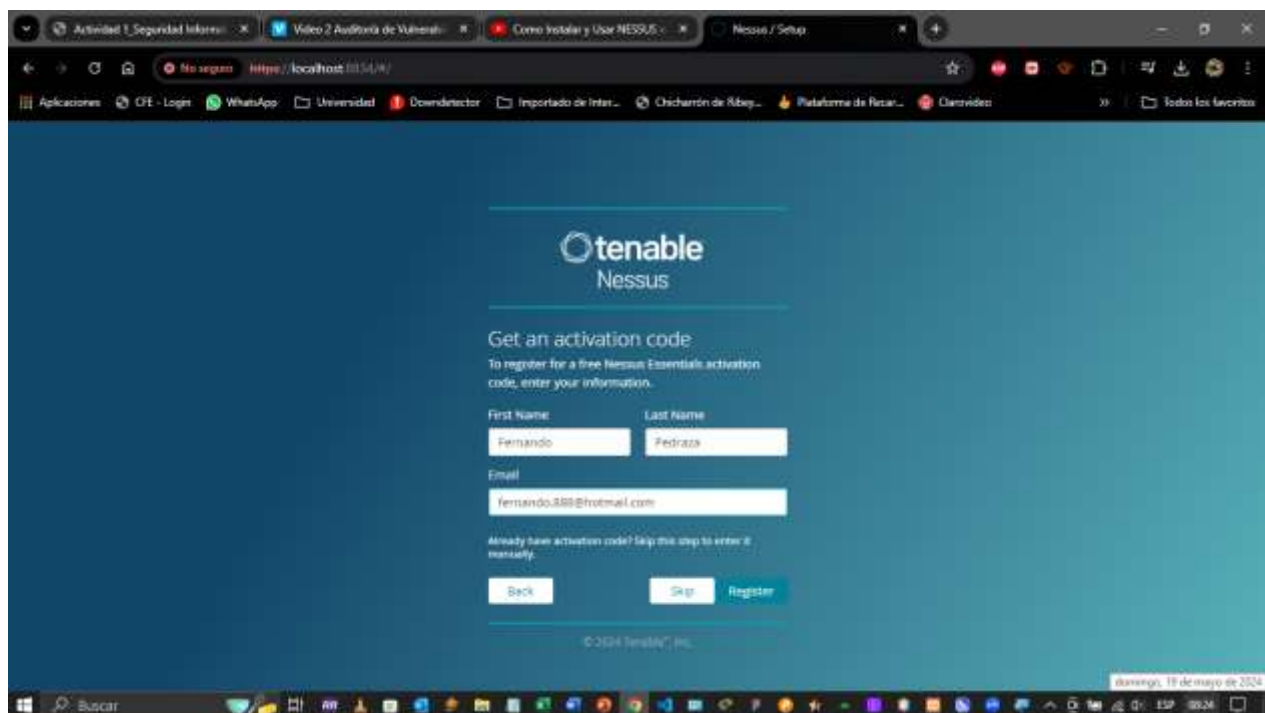
Al concluir se hace la conexión vía SSL con nessus



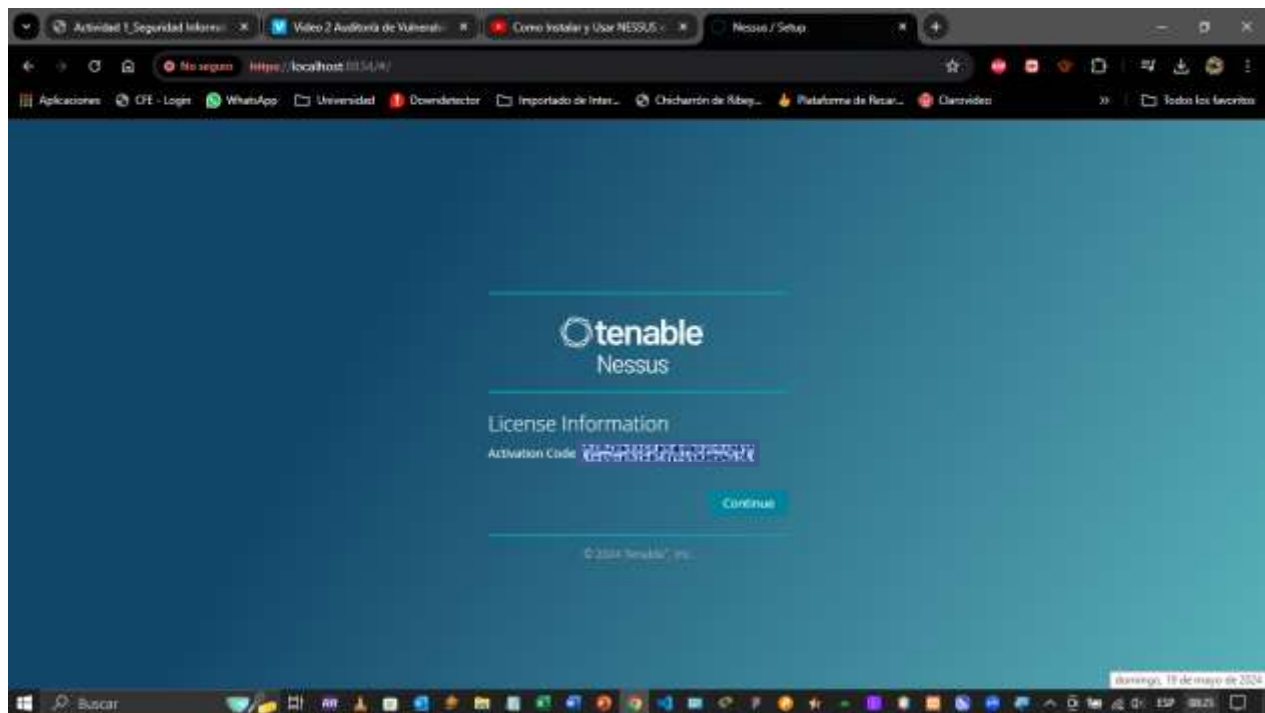
Se continua con el registro en línea



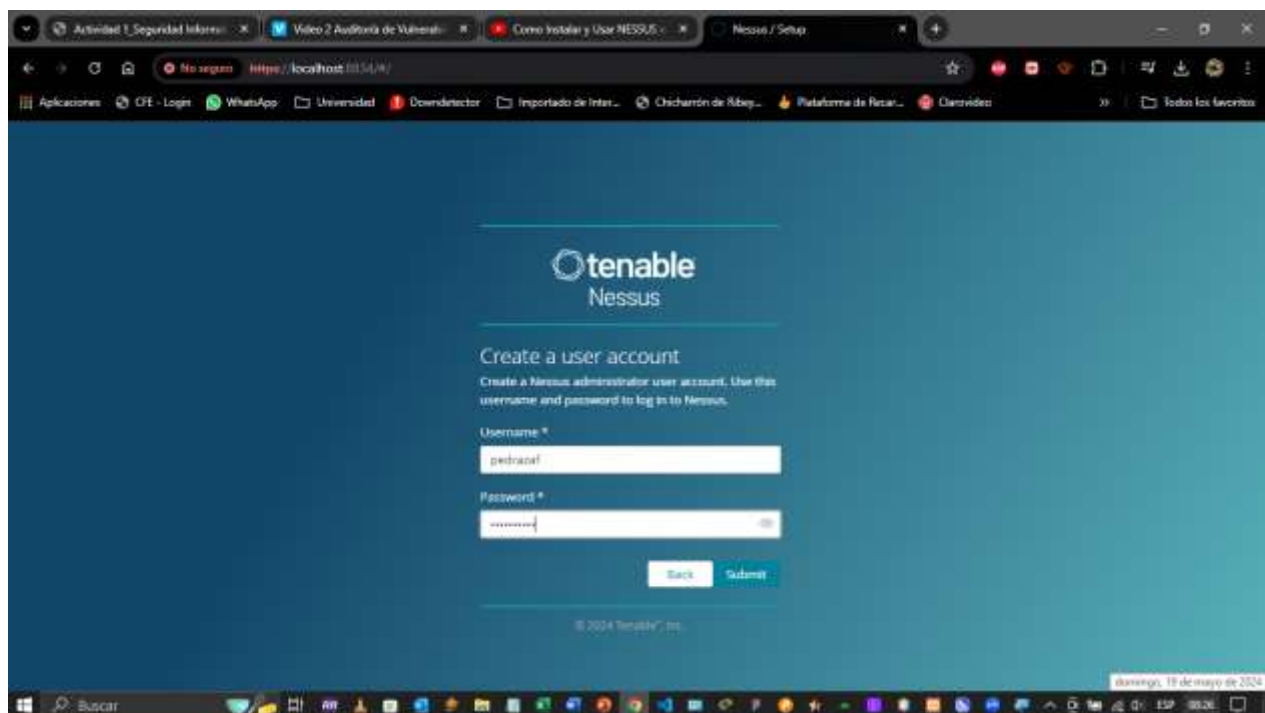
Se selecciona el registro para Nessus Essentials



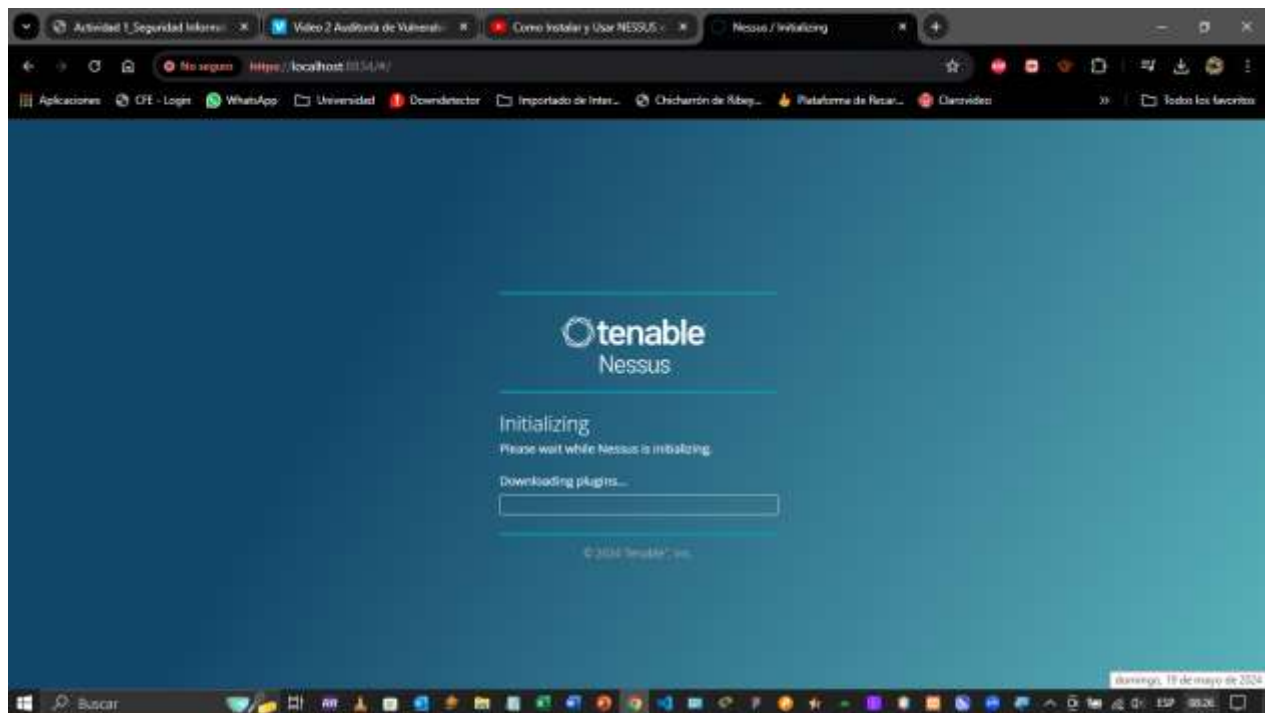
Se registran los datos solicitados



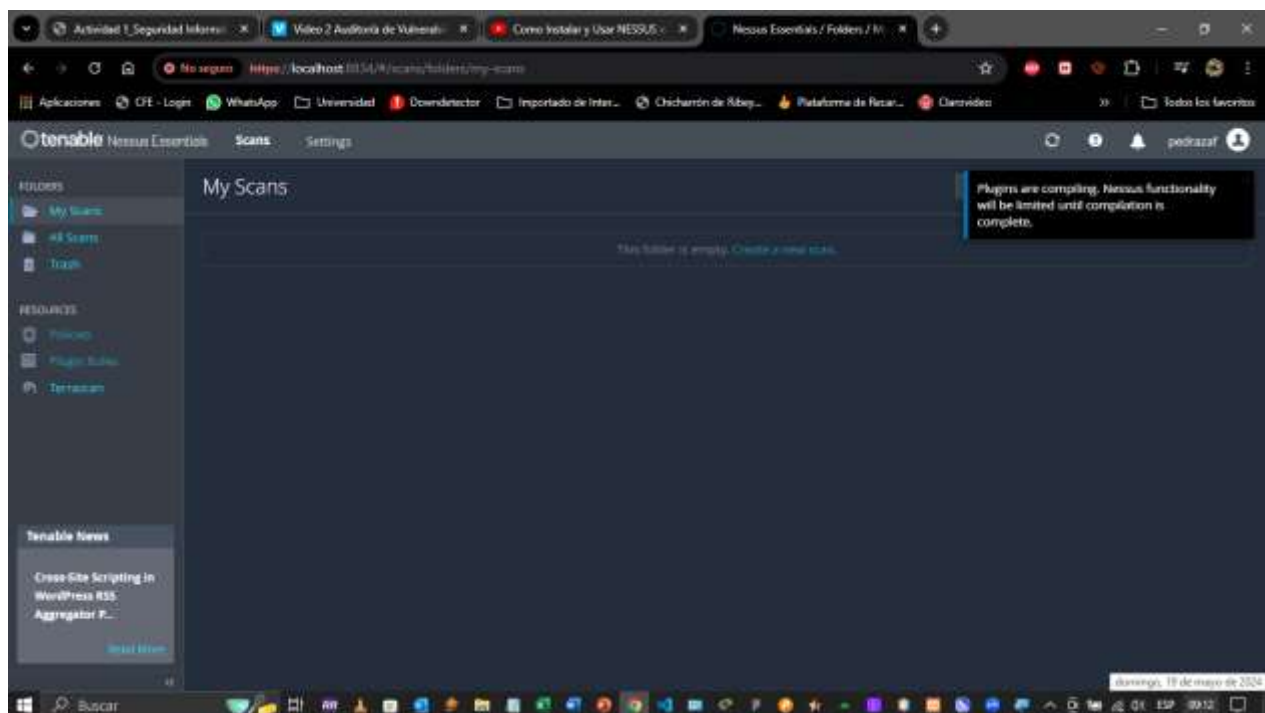
Muestra el código de activación



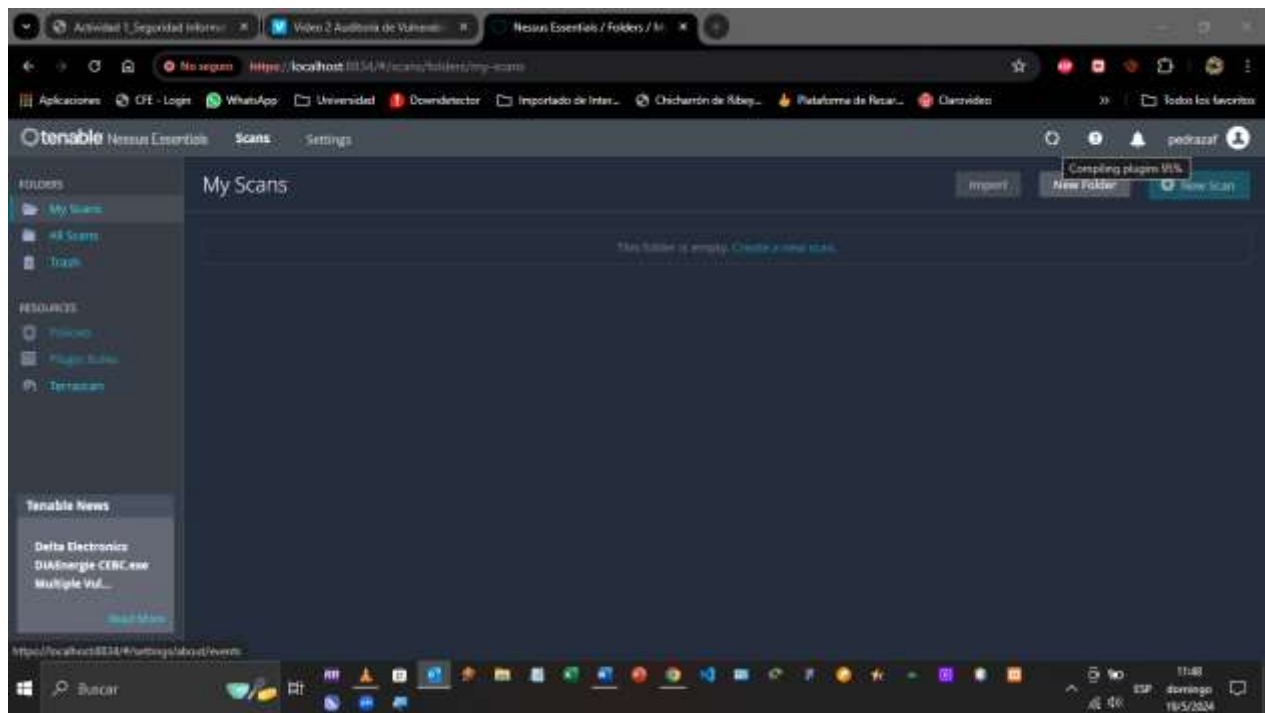
Se crea un usuario y una contraseña robusta



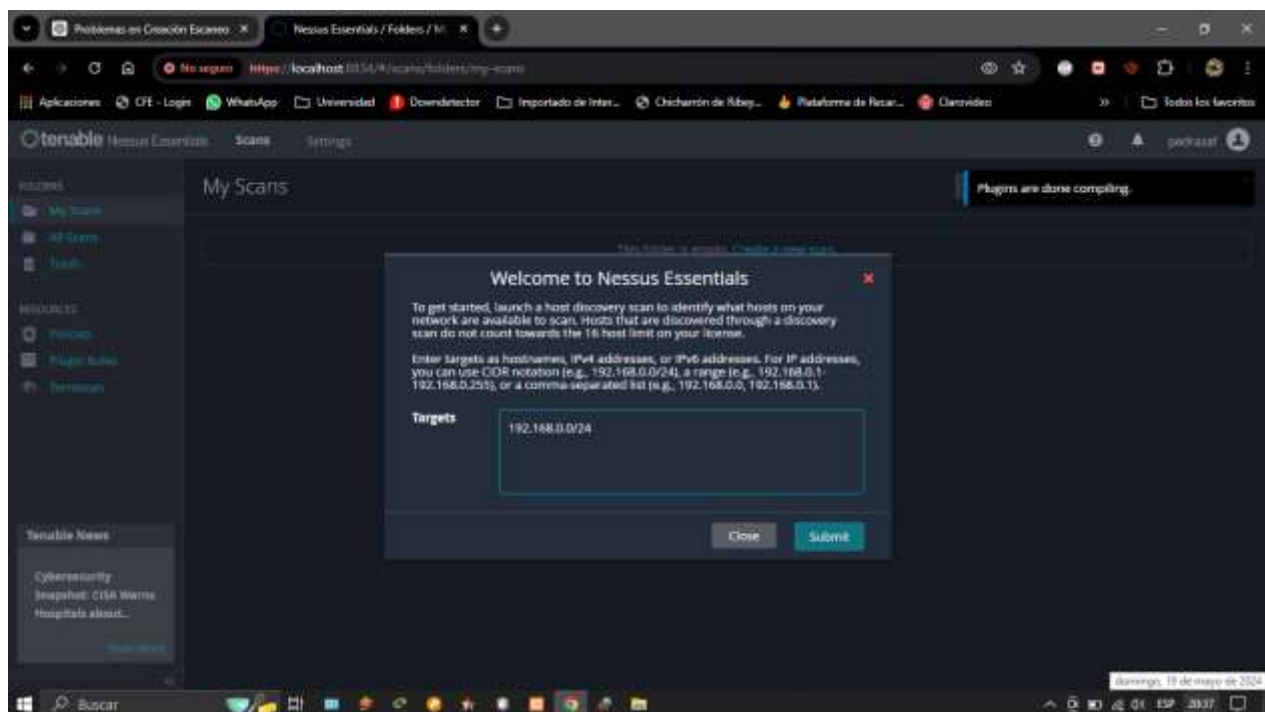
Comienza la instalación

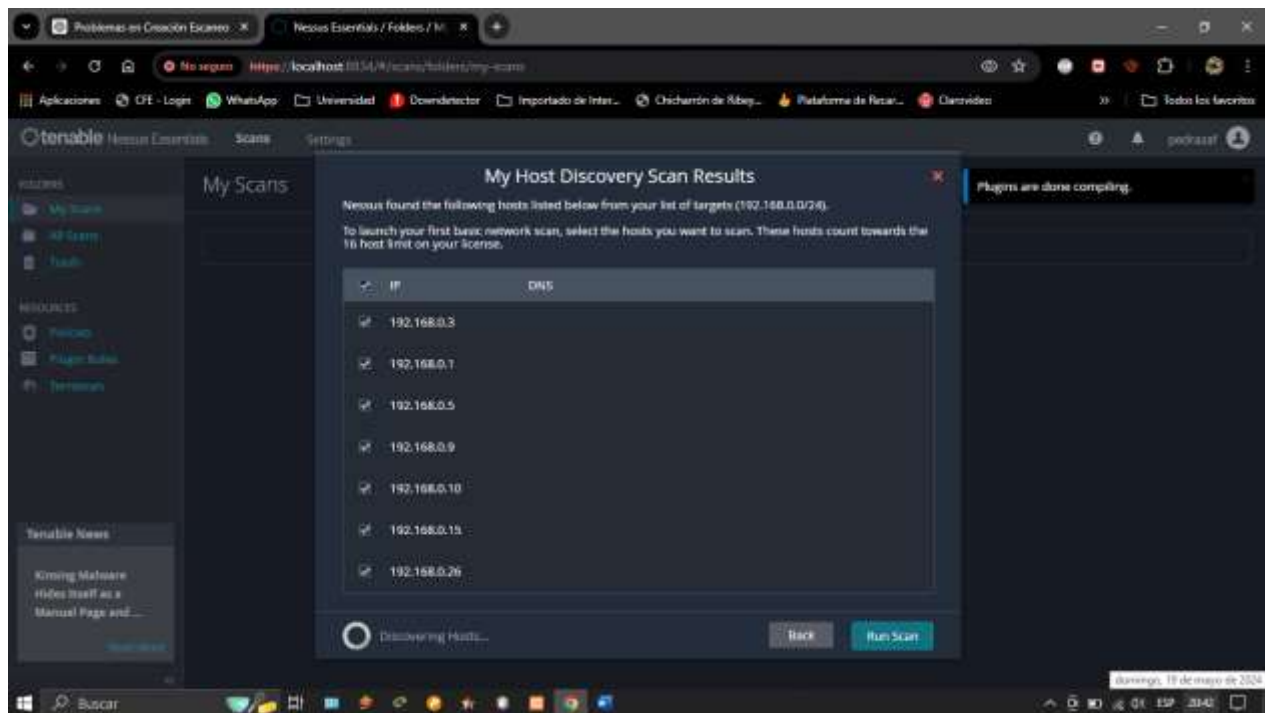


Al concluir se abre la plataforma compilando los plugins para su buen funcionamiento



Una vez concluidos se crea un nuevo escaneo en búsqueda de posibles ataques como son virus, accesos no permitidos o percances de red.





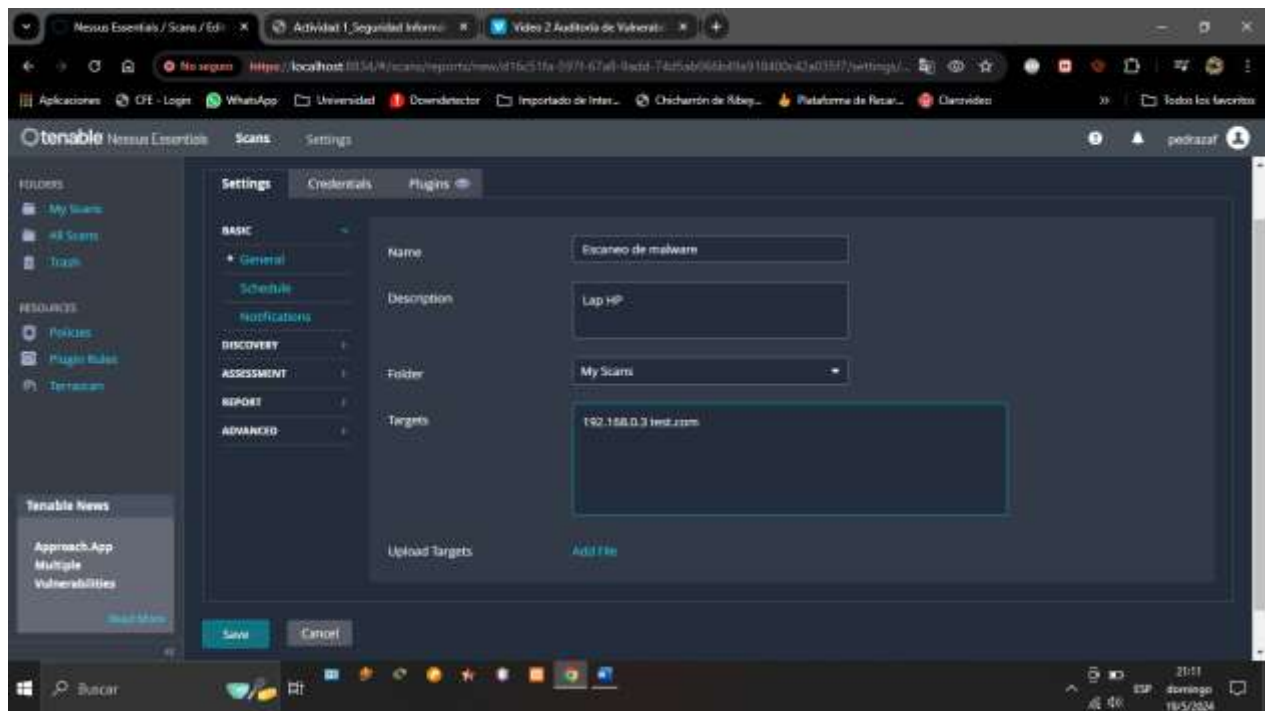
Escaneando los dispositivos que están conectados a la red

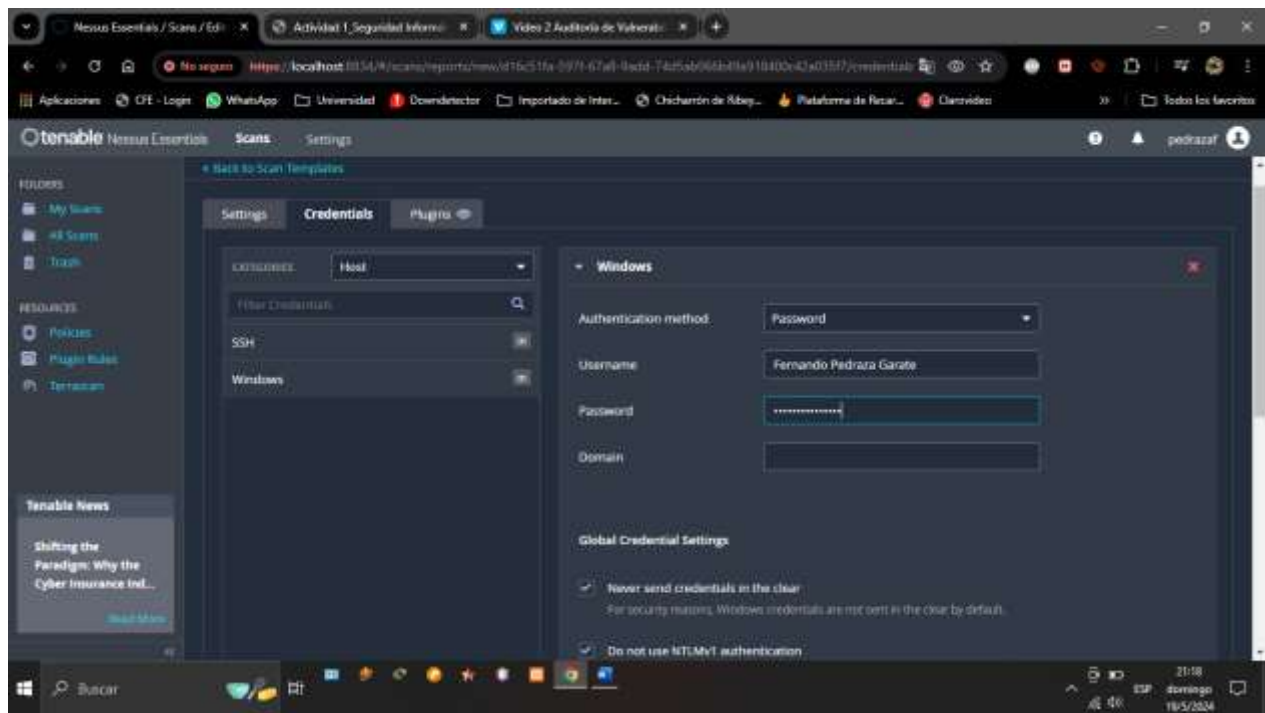


Mostrando el estatus de vulnerabilidad de cada dispositivo conectado a la red

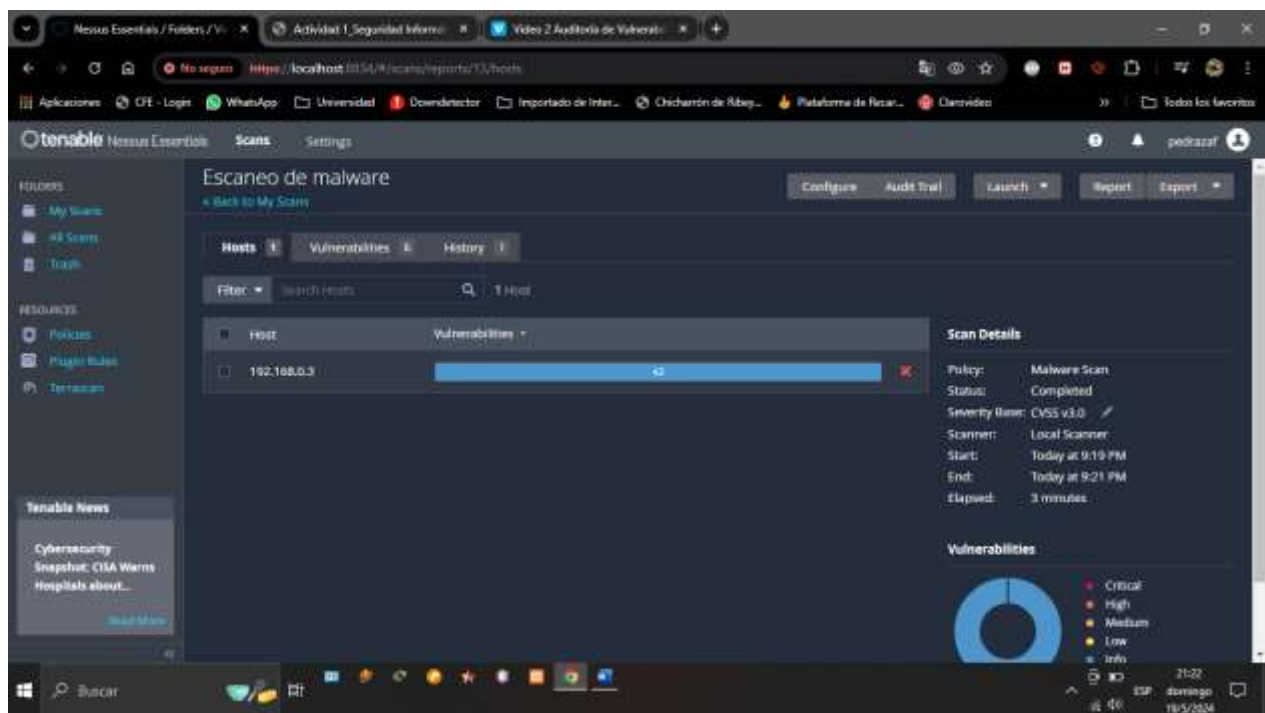


Se crea un nuevo escaneo en busca de malware

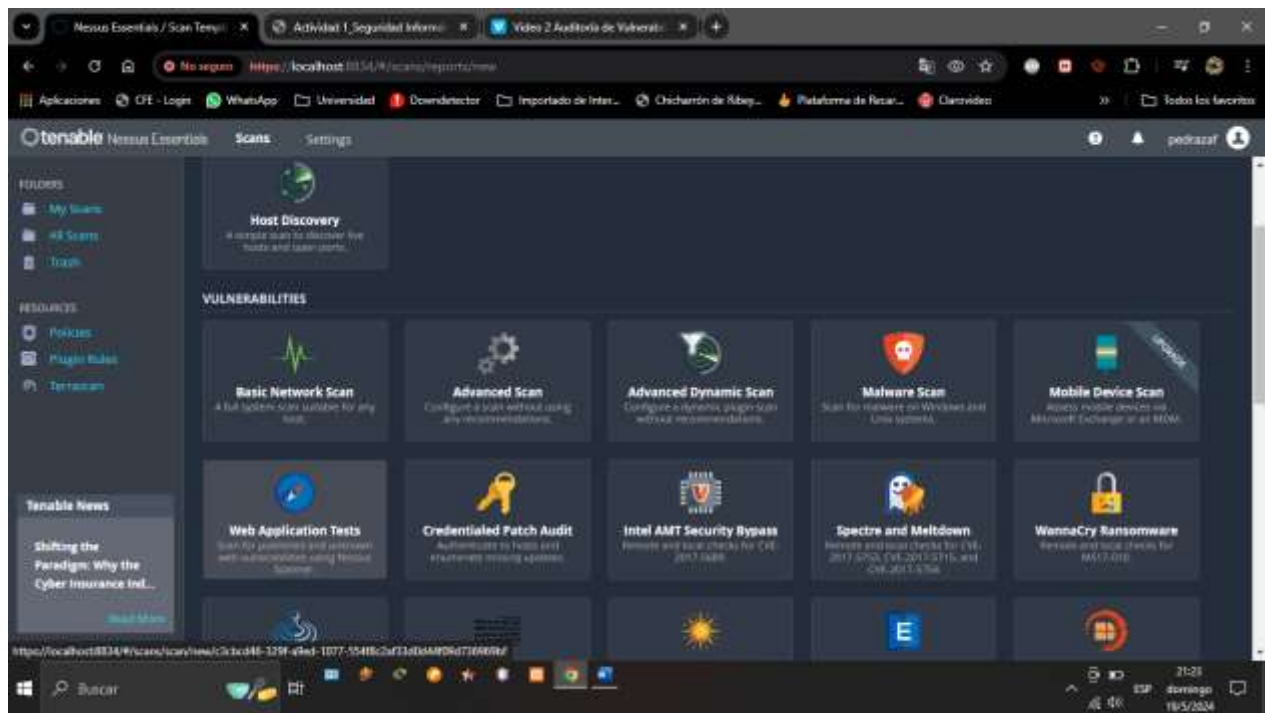




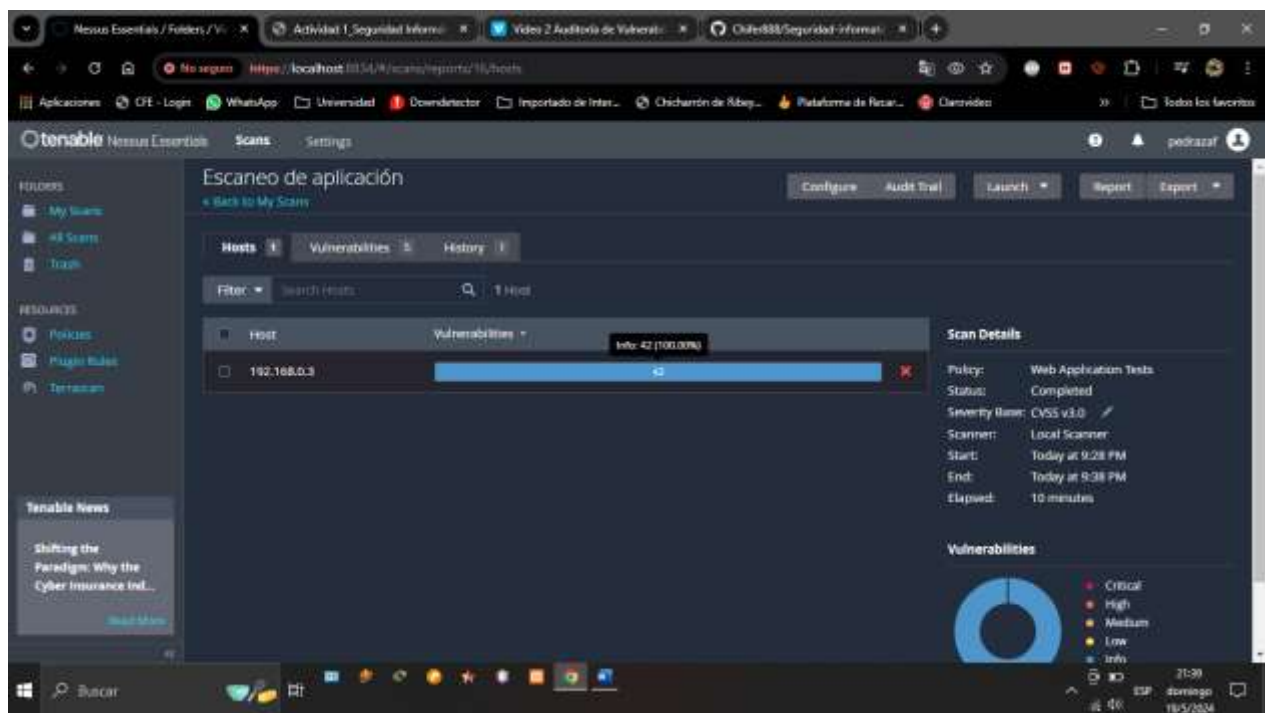
Se ingresan las credenciales y se ejecuta el programa



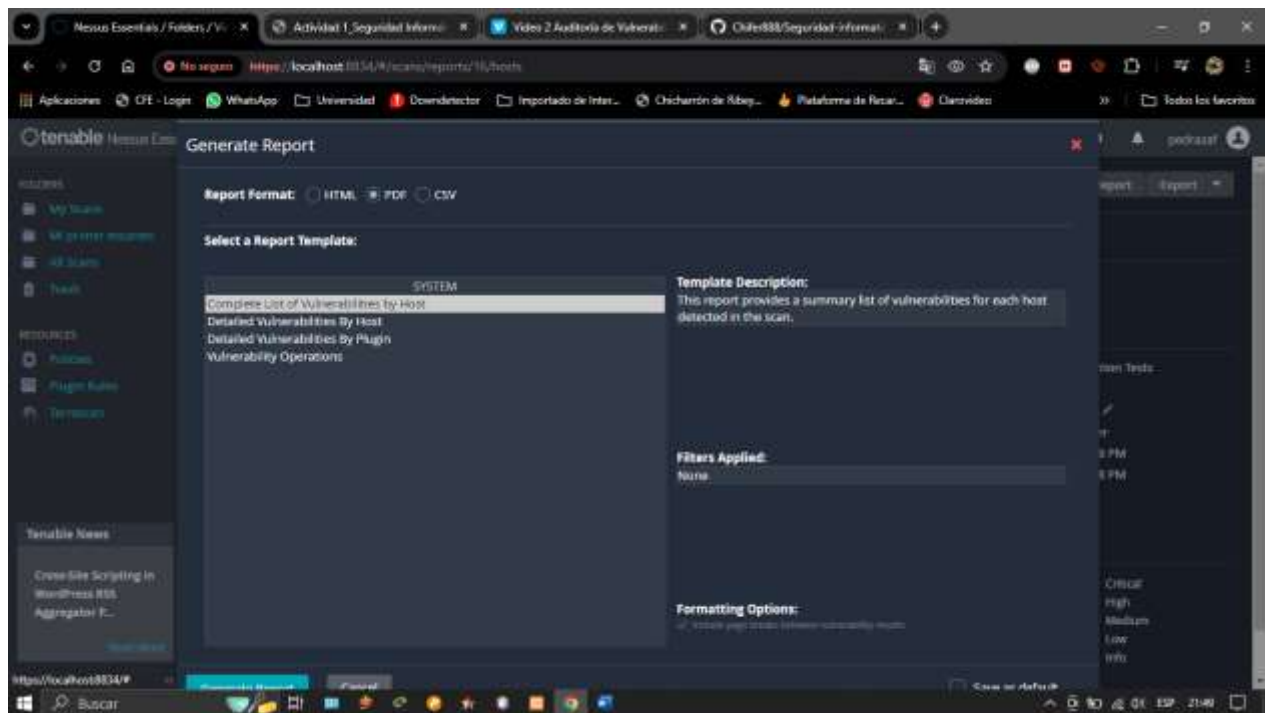
Mostrando los resultados del análisis al terminar el escaneo



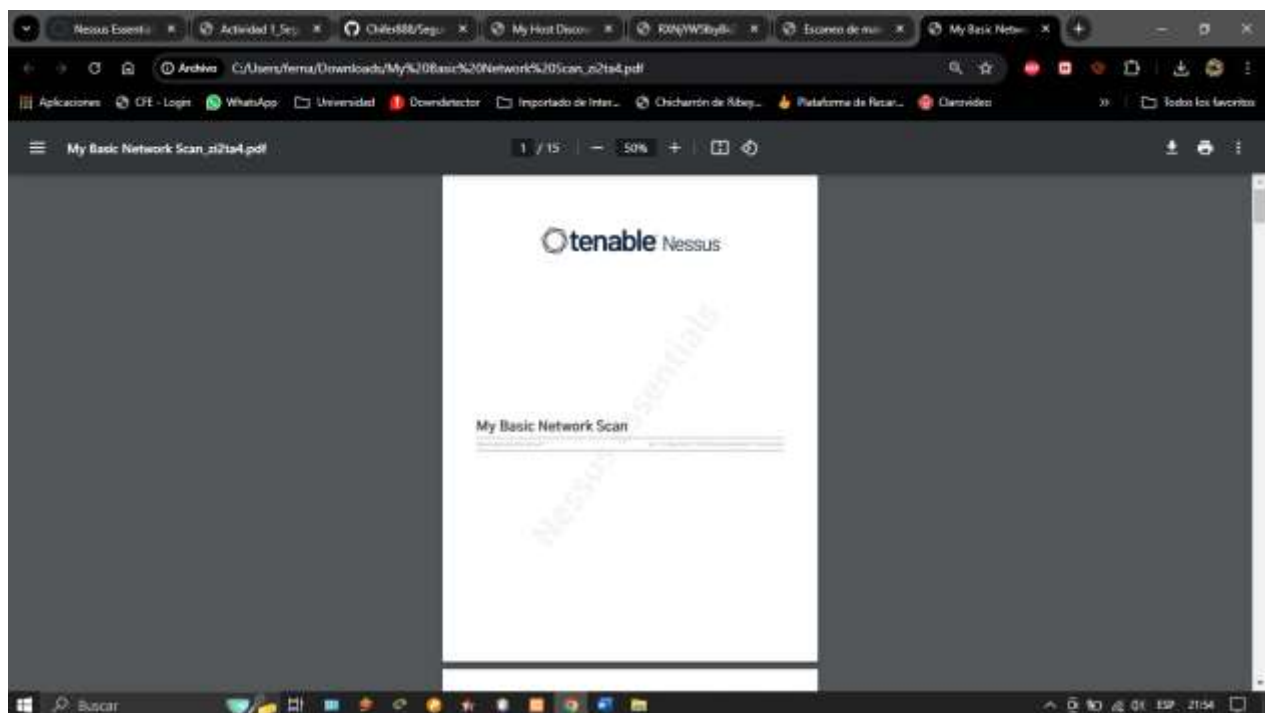
Se crea un escaneo de aplicación web para detectar vulnerabilidades de navegación.



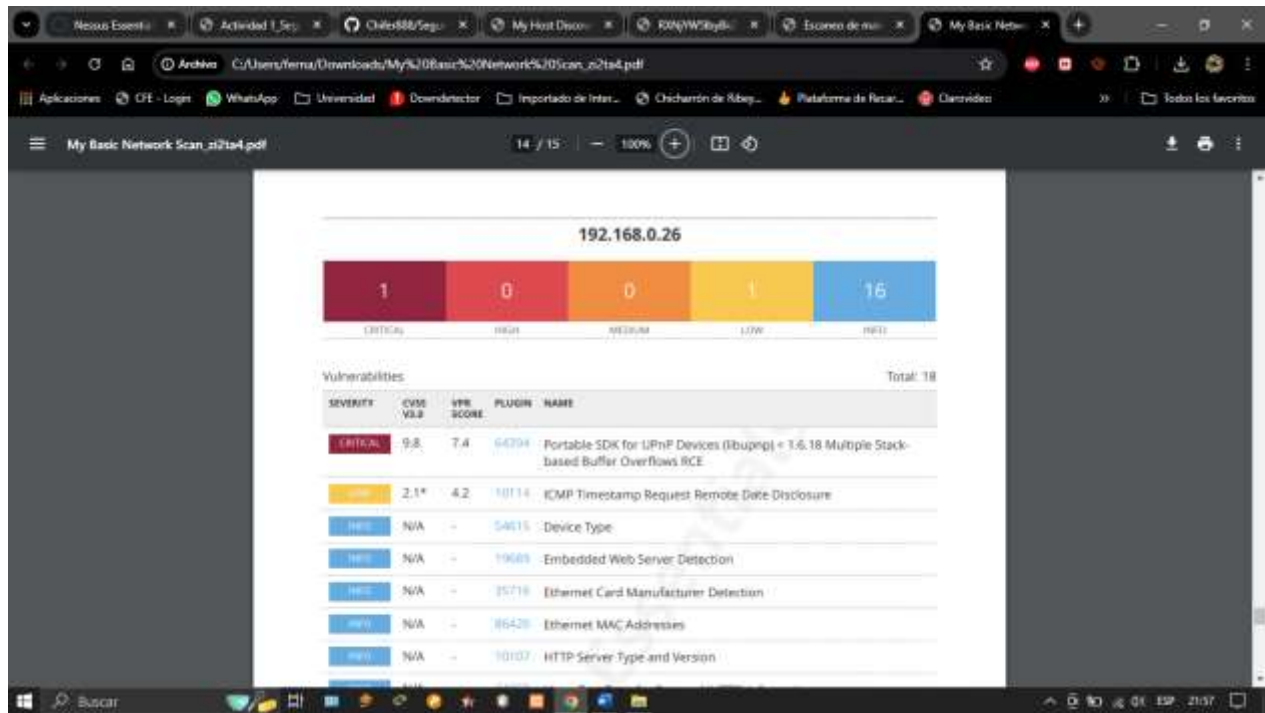
Mostrando los resultados al final del escaneo

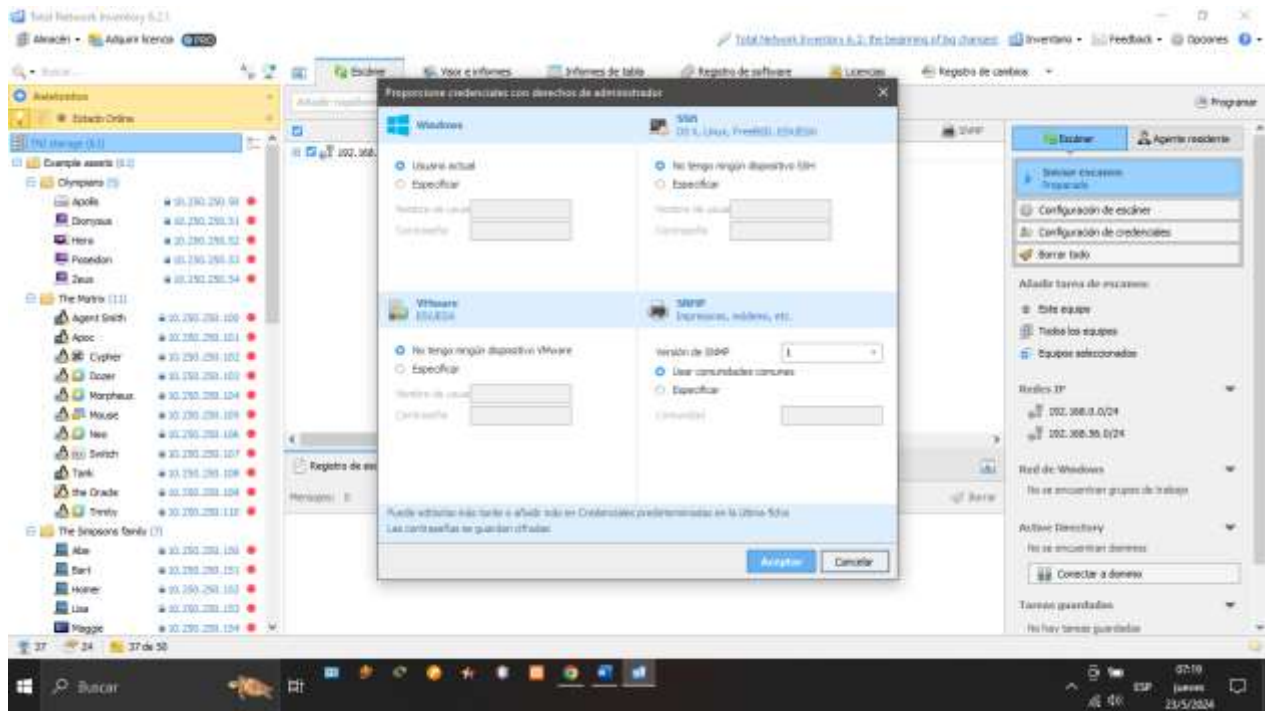


Se crean los reportes en el formato deseado como PDF, HTML o CSV

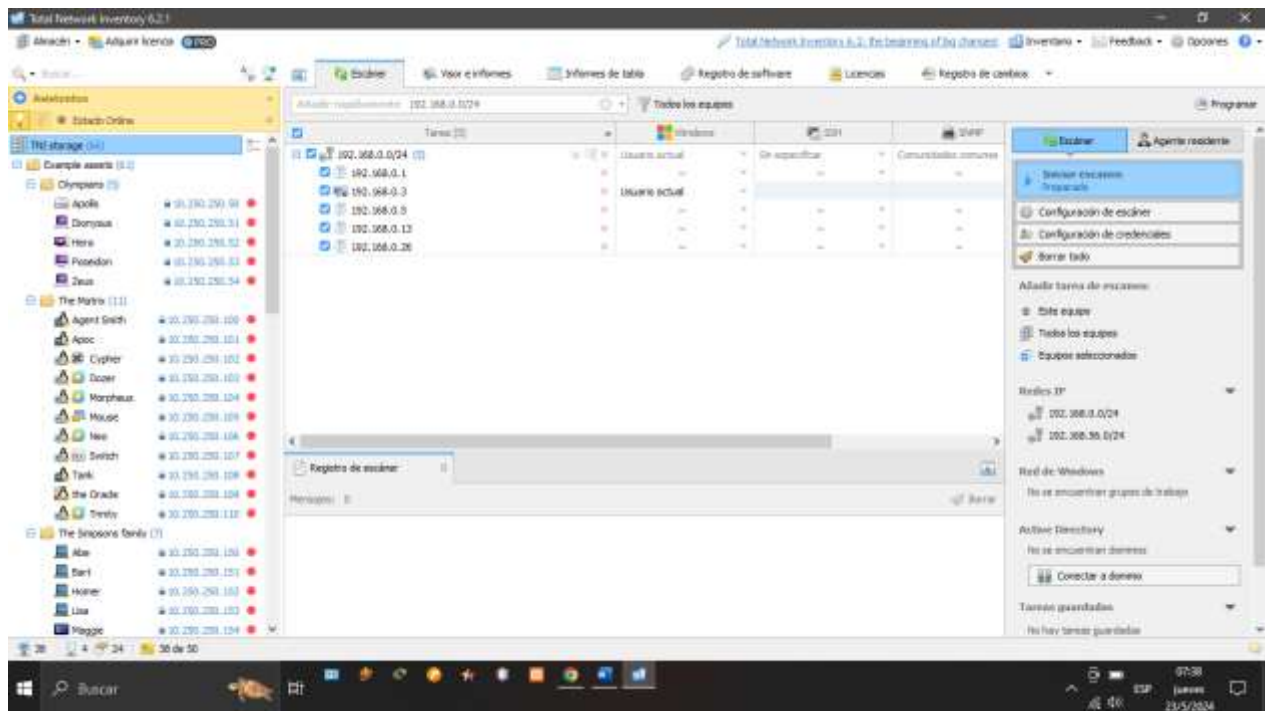


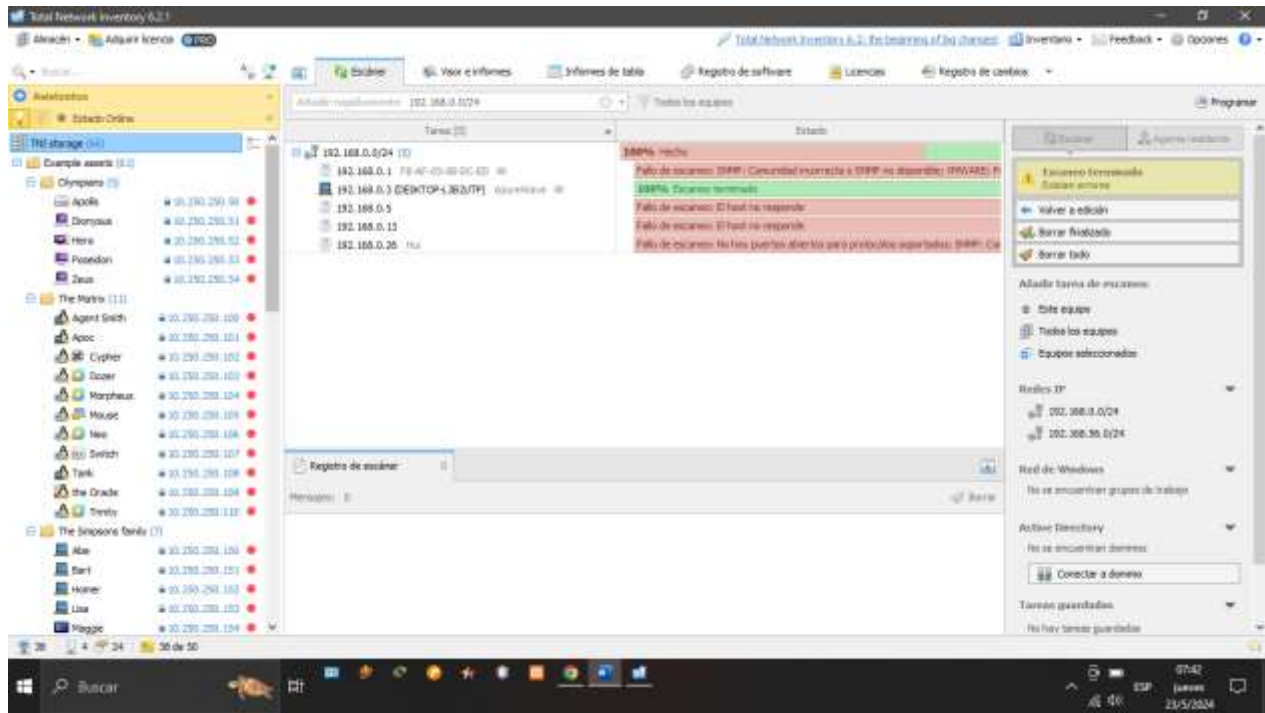
Mostrando un informe detallado de las vulnerabilidades encontradas por dispositivo y sus detalles



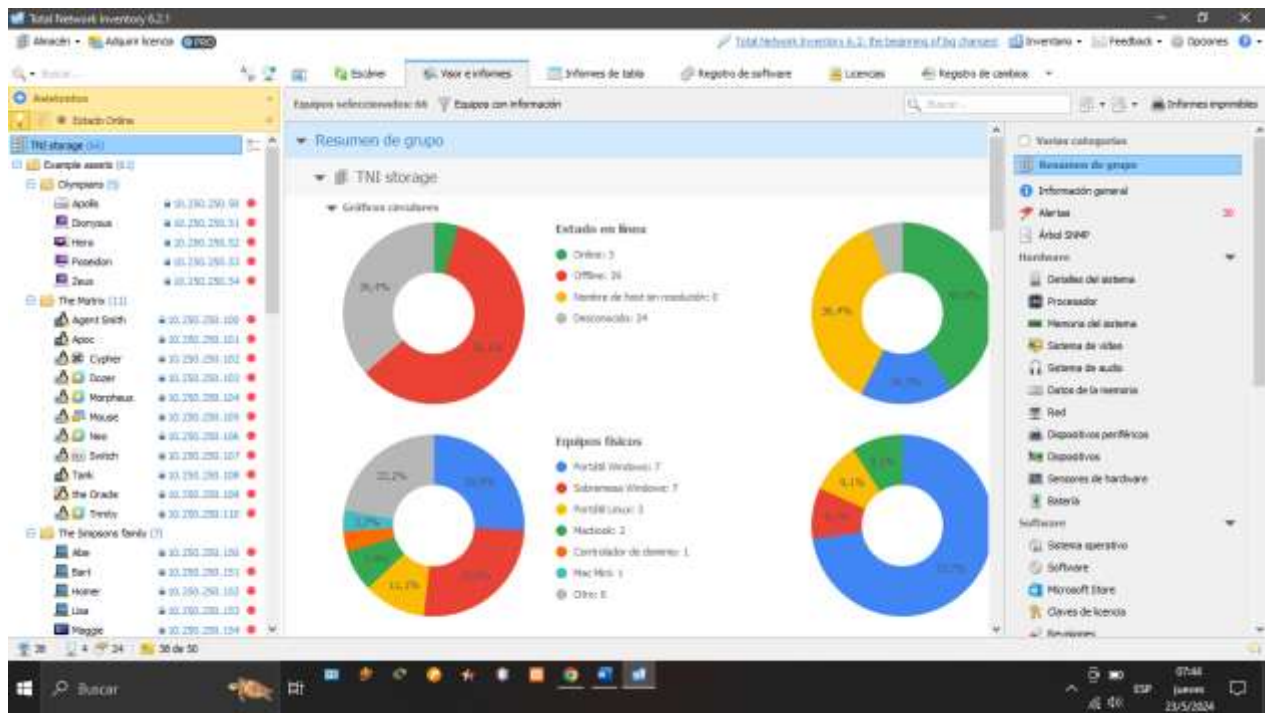


Se inicia el escaneo rápido proporcionando credenciales de administrador

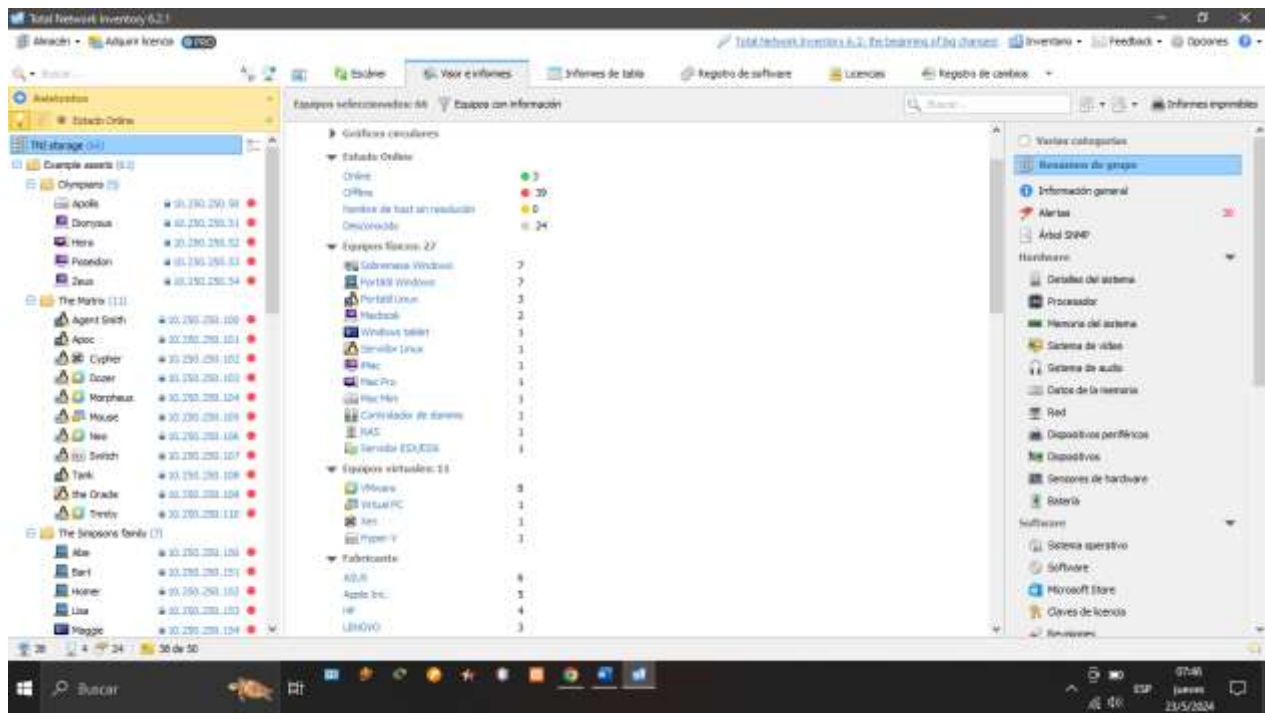




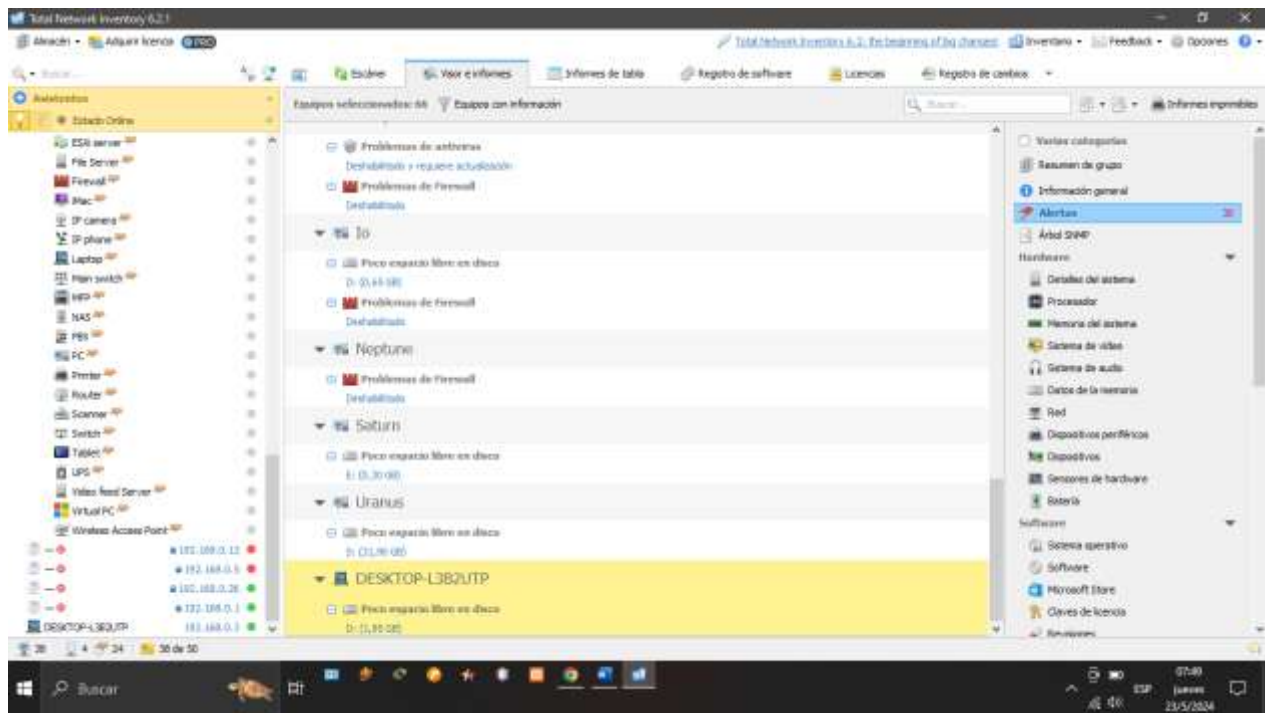
Se hace el escaneo preparado y al finalizar muestra si es que existen errores.

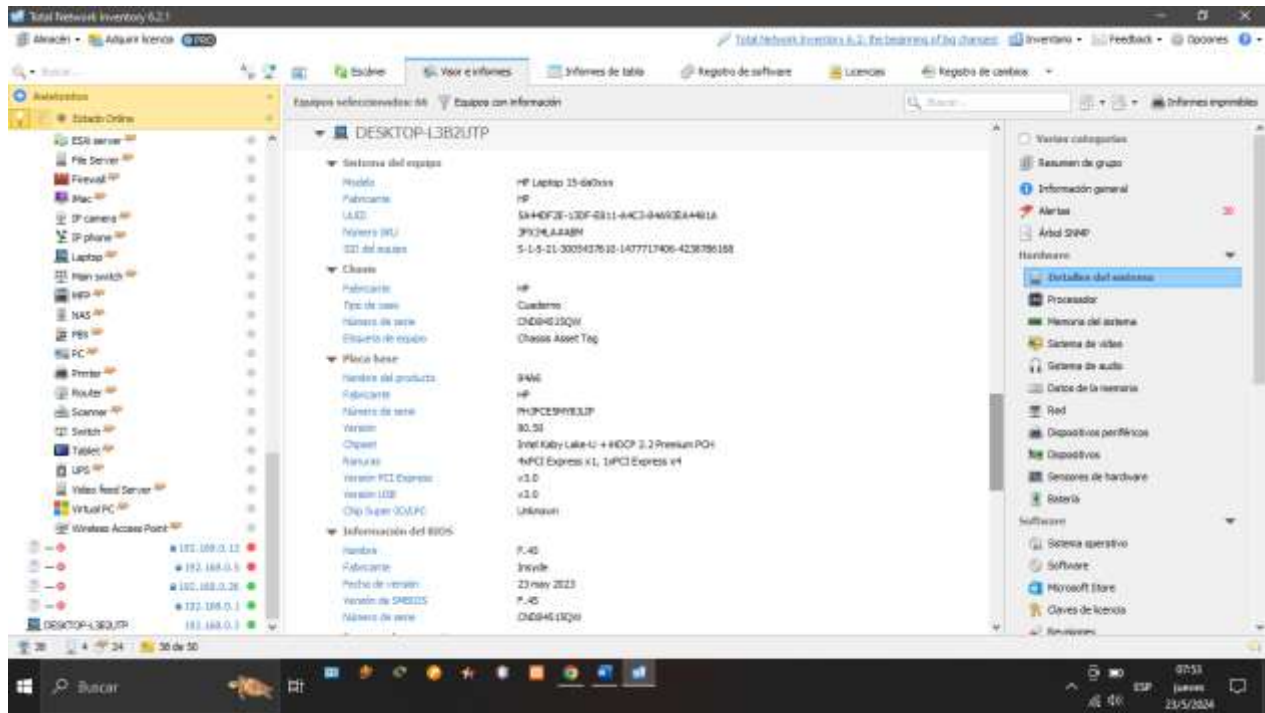


Mostrando de forma grafica el estado de la red en general

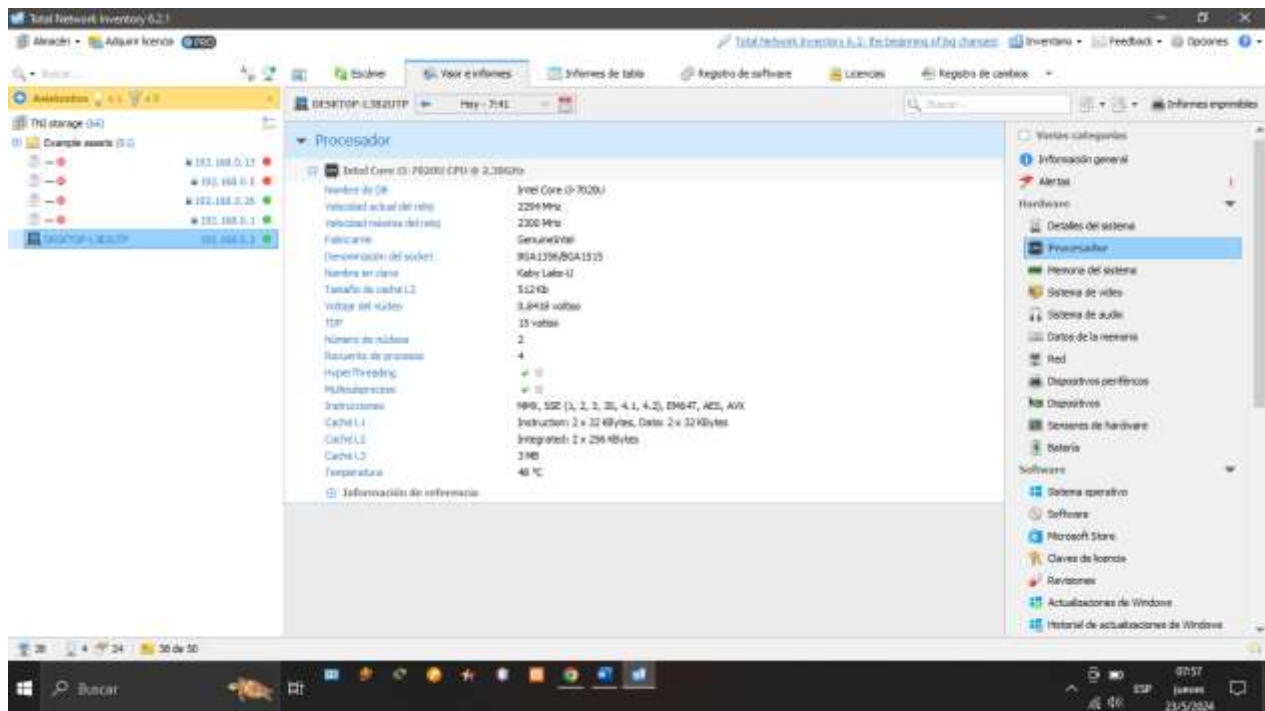


Mostrando los equipos en línea

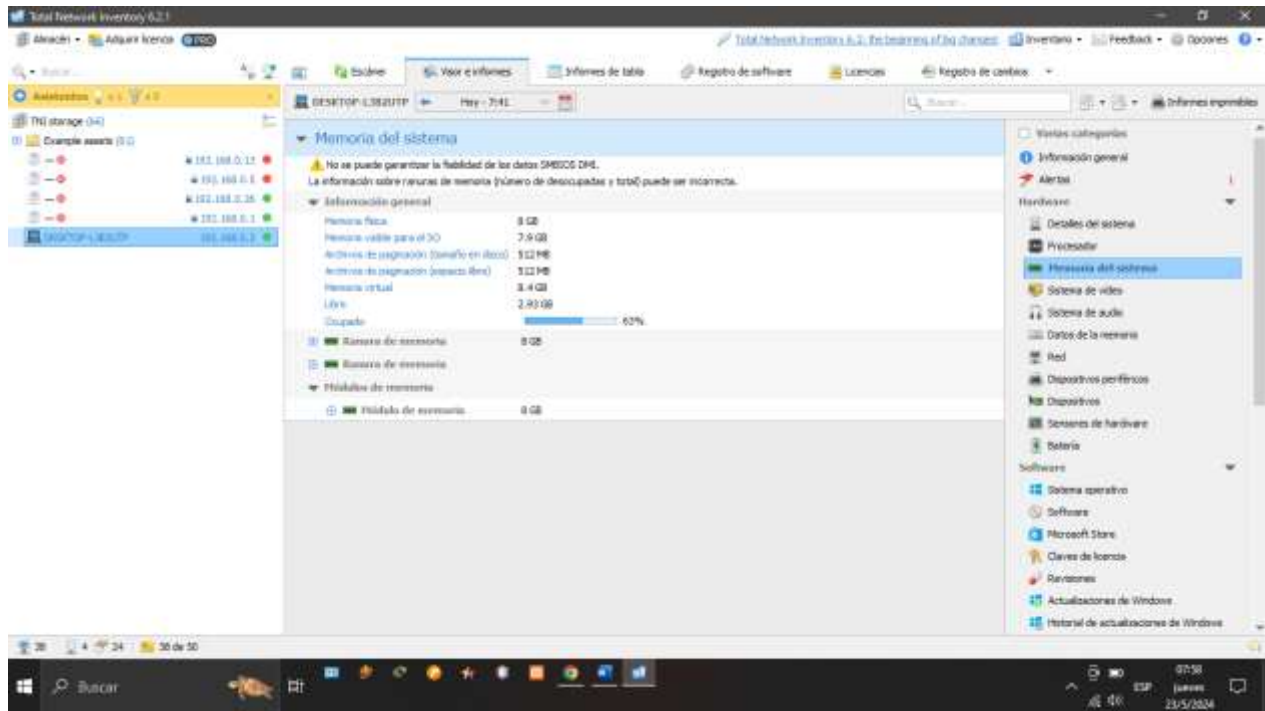




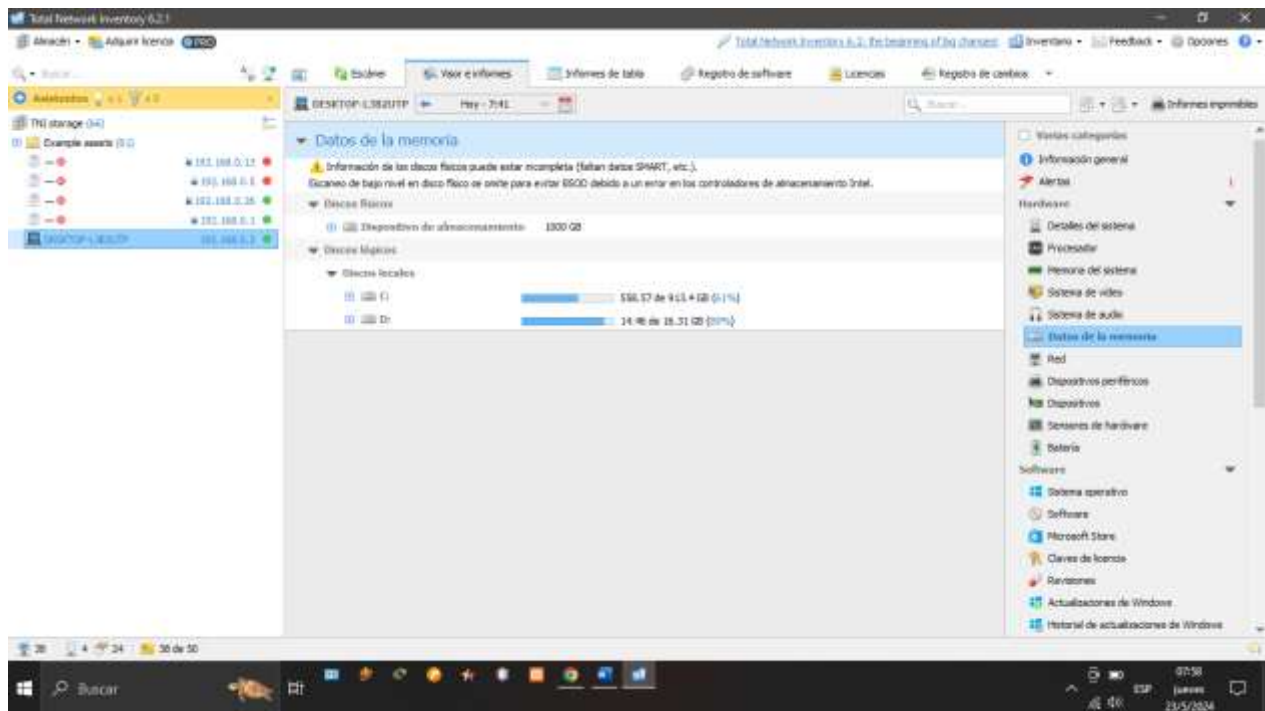
Como parte de auditoria se puede gestionar el hardware del equipo conectado a la red



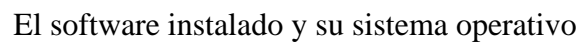
Mostrando los datos del procesador

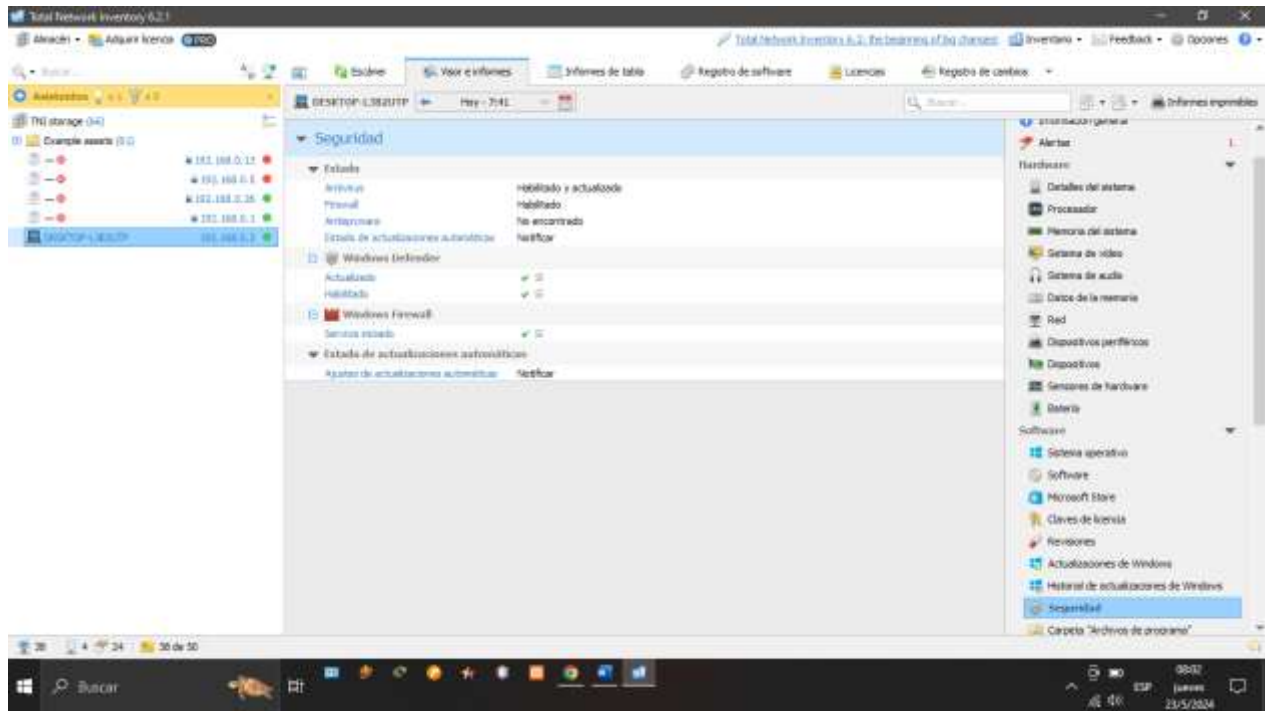


La memoria que tiene el sistema

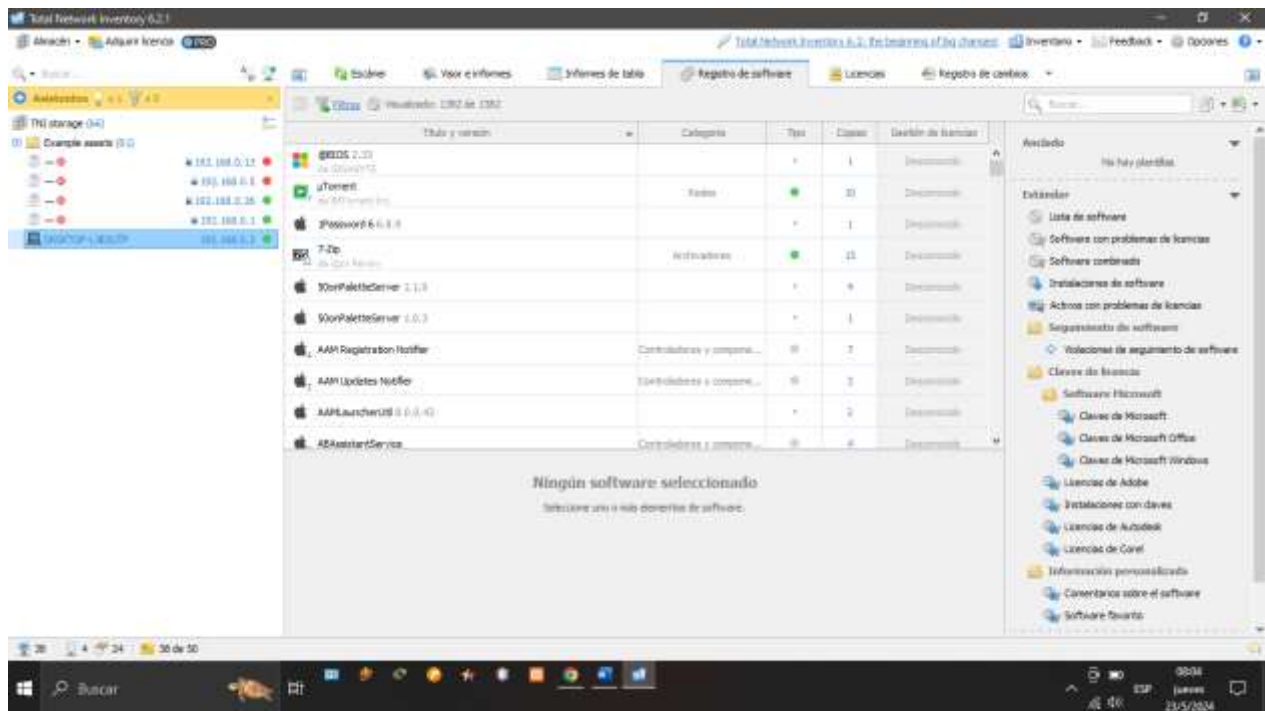


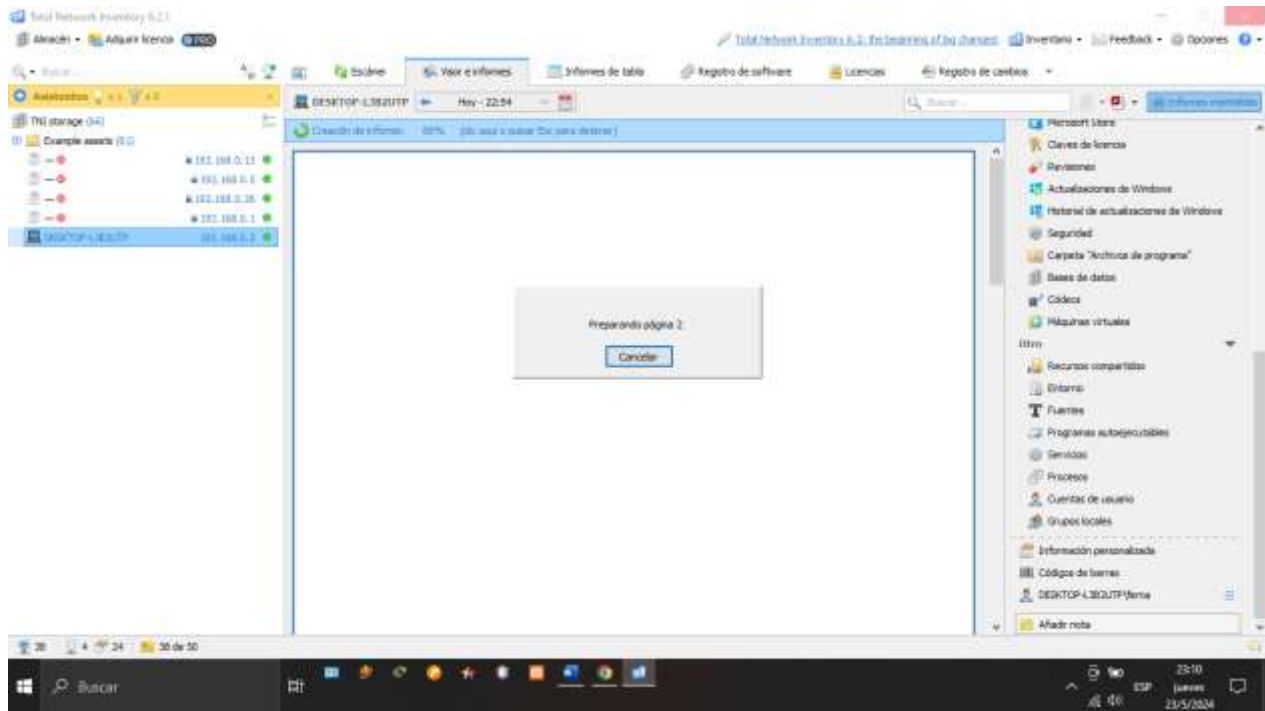
Los datos de la memoria física



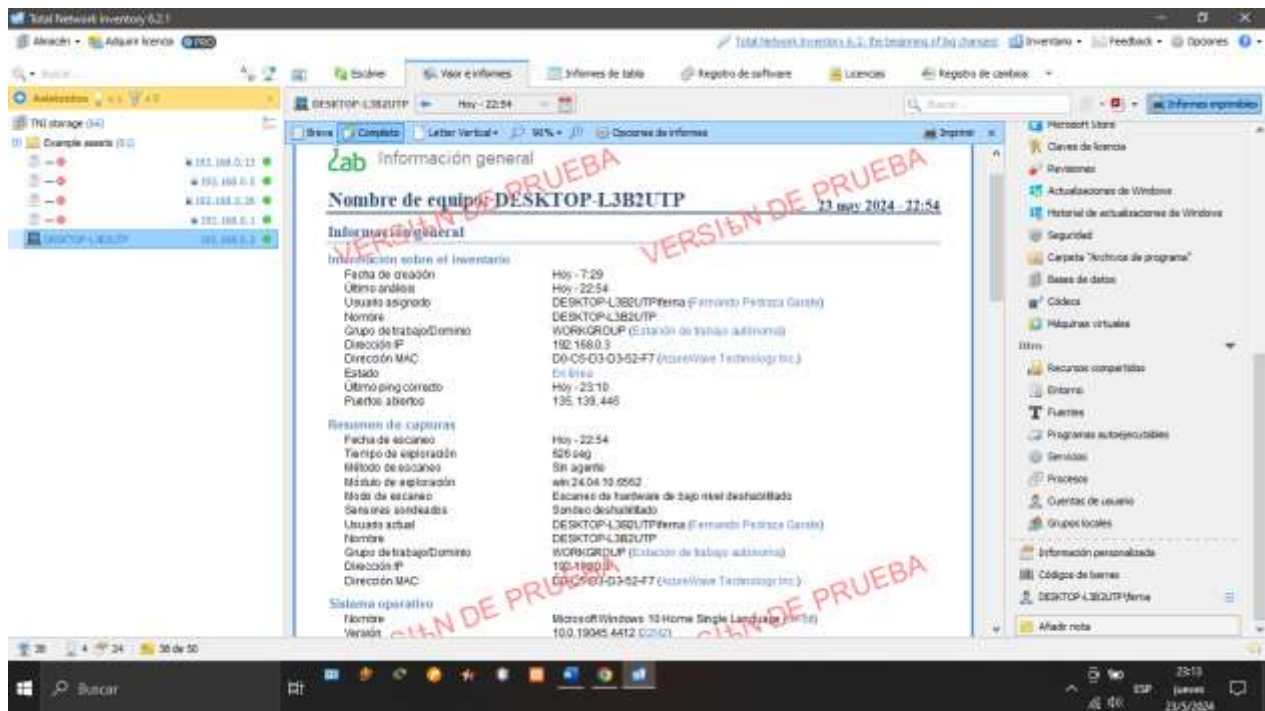


La seguridad presentada en los equipos conectados

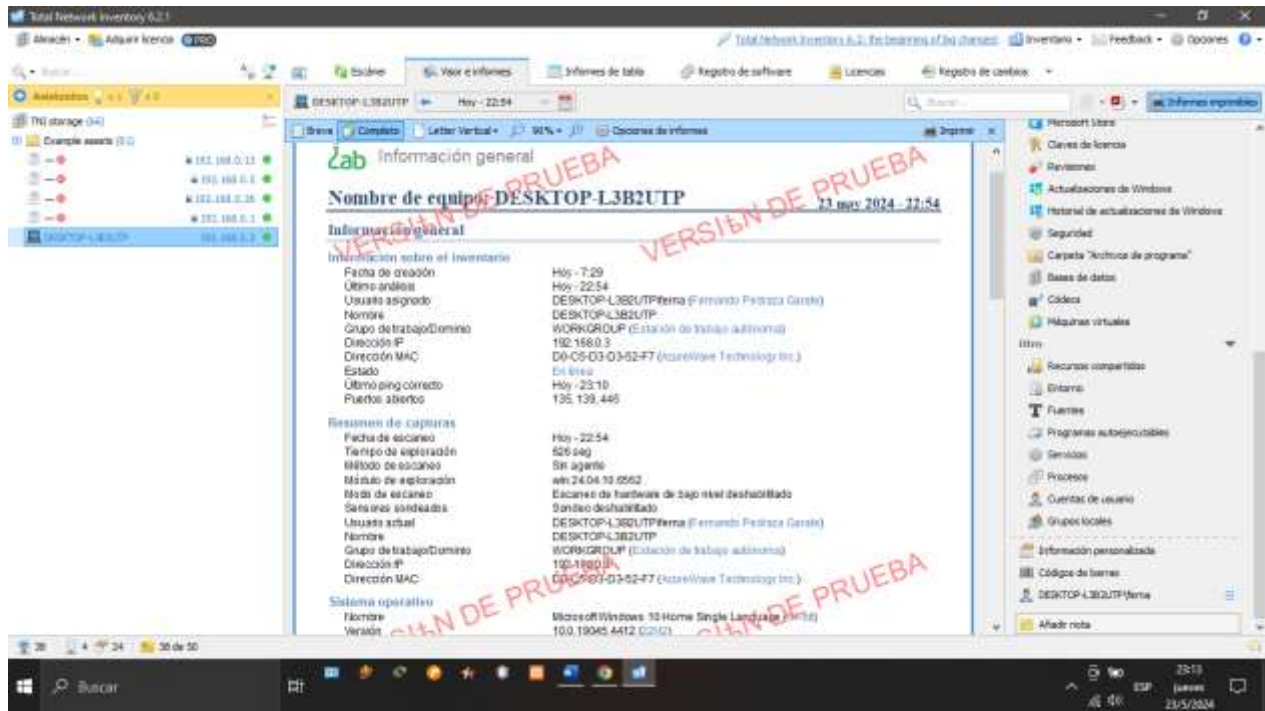




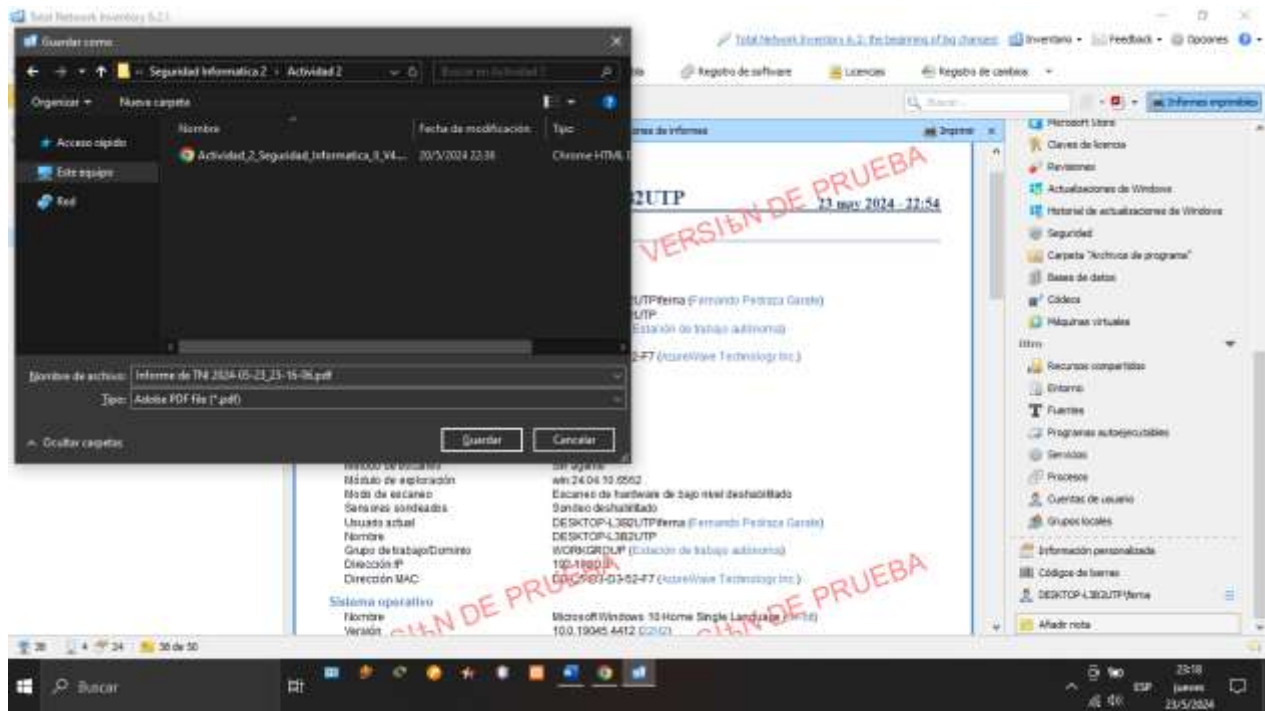
Se genera el reporte imprimible

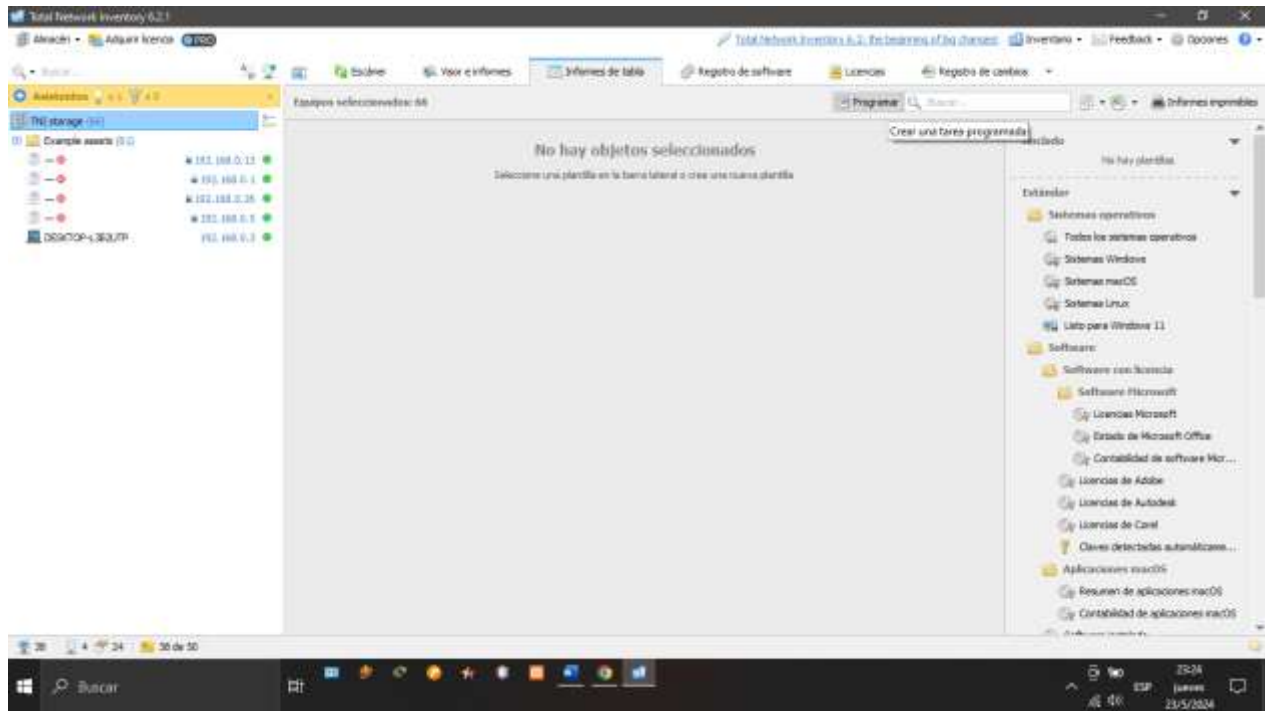


Mostrando toda la información relacionada con la seguridad del dispositivo auditado.

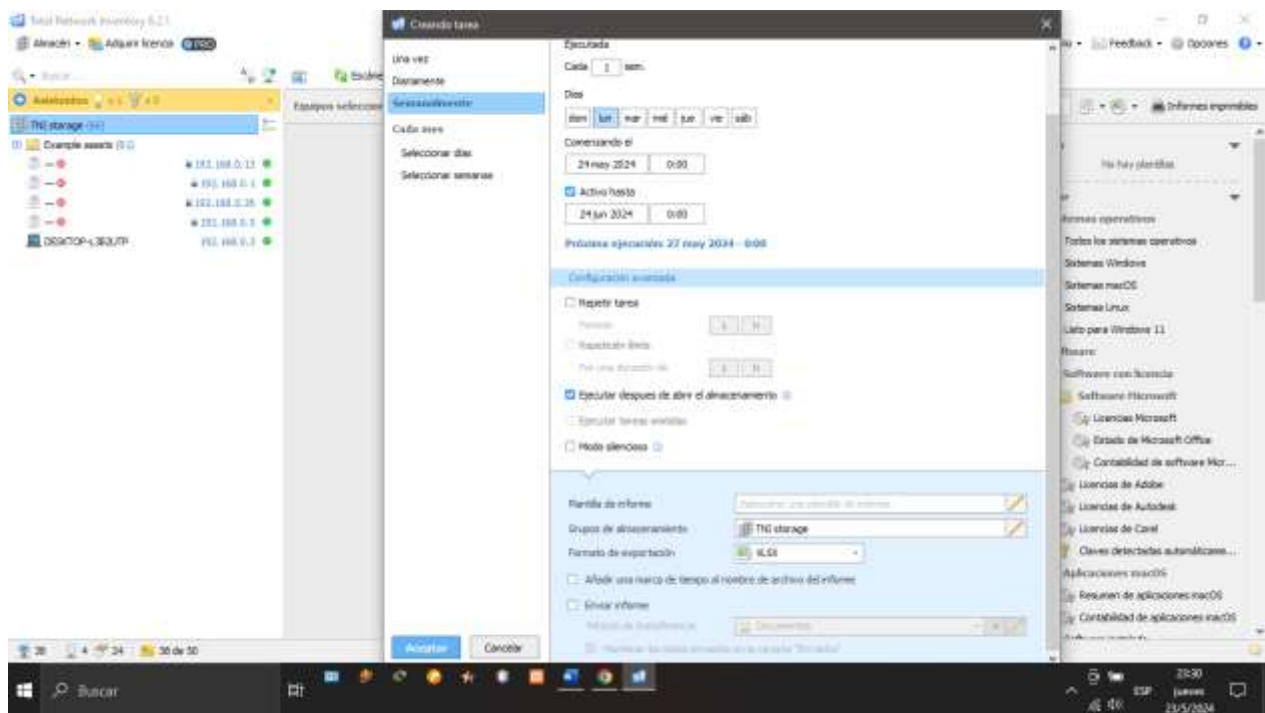


Guardando el reporte en formato PDF en el dispositivo

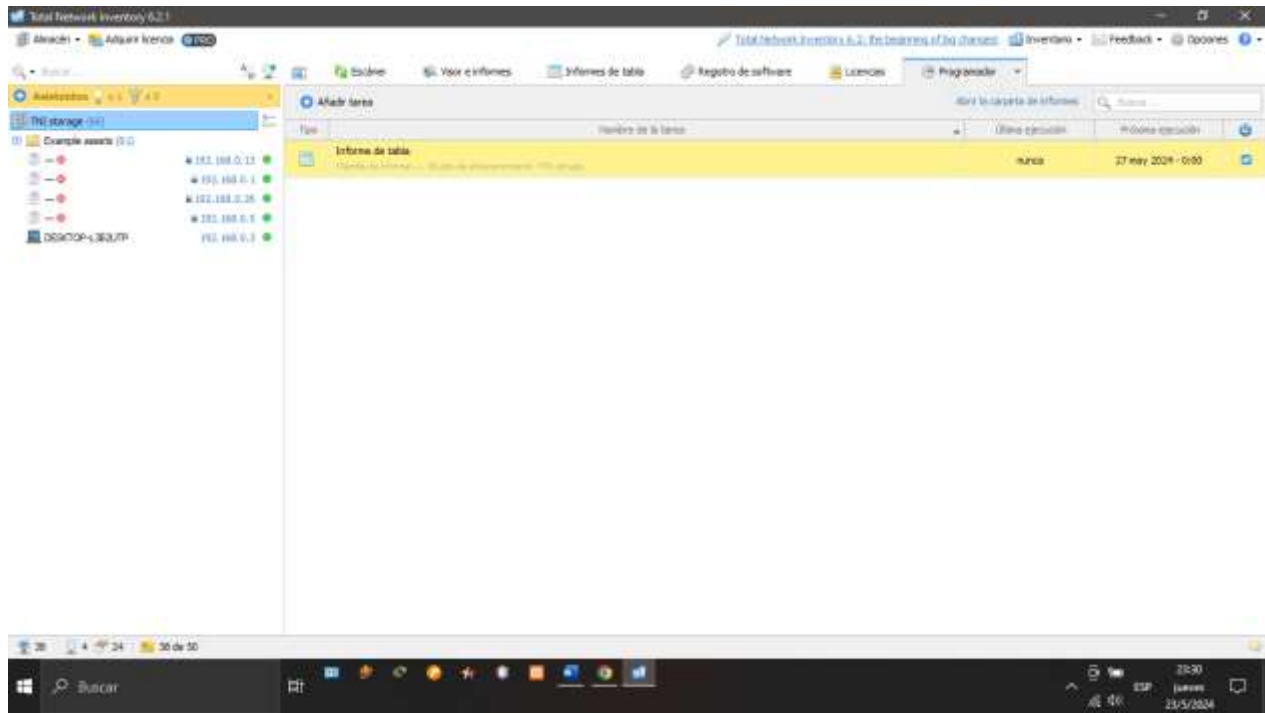




Se programa una auditoria semanal posterior al primer escaneo

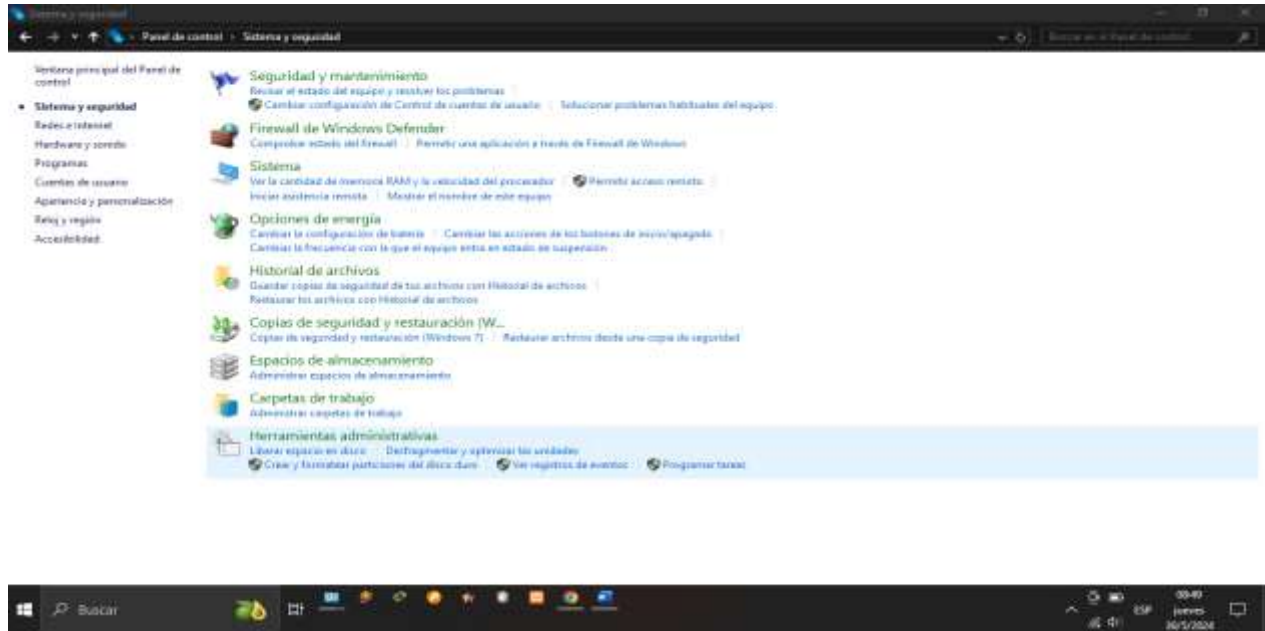


Ingresando el tiempo de vigencia para el escaneo programado y se guarda

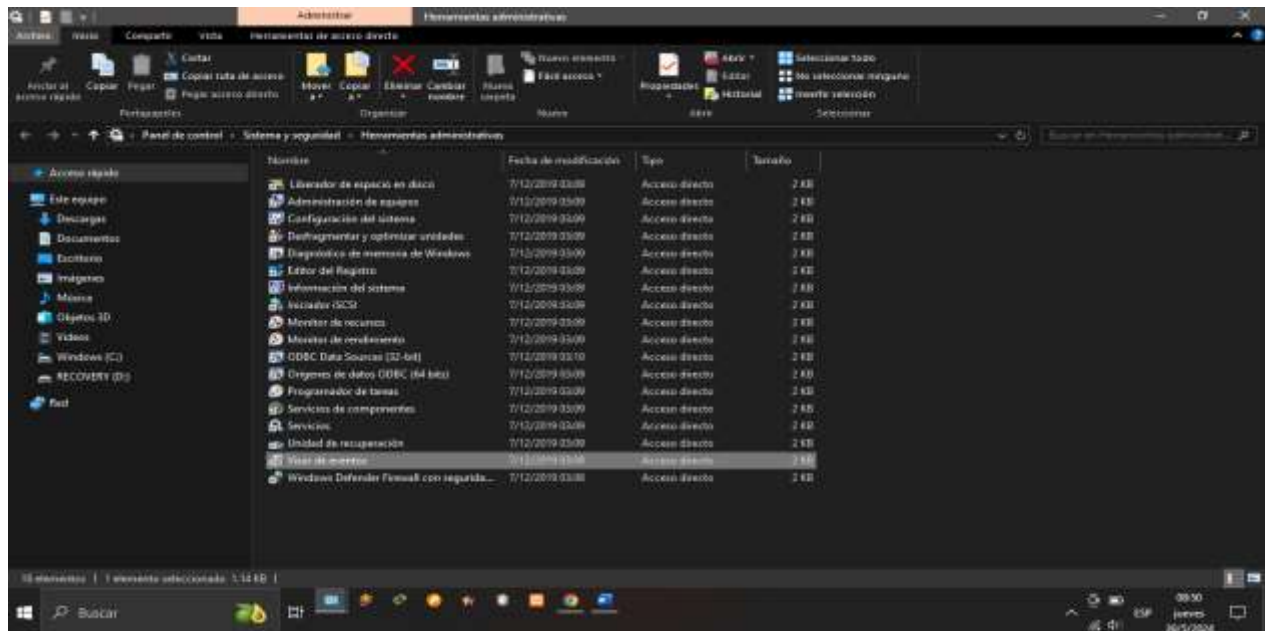


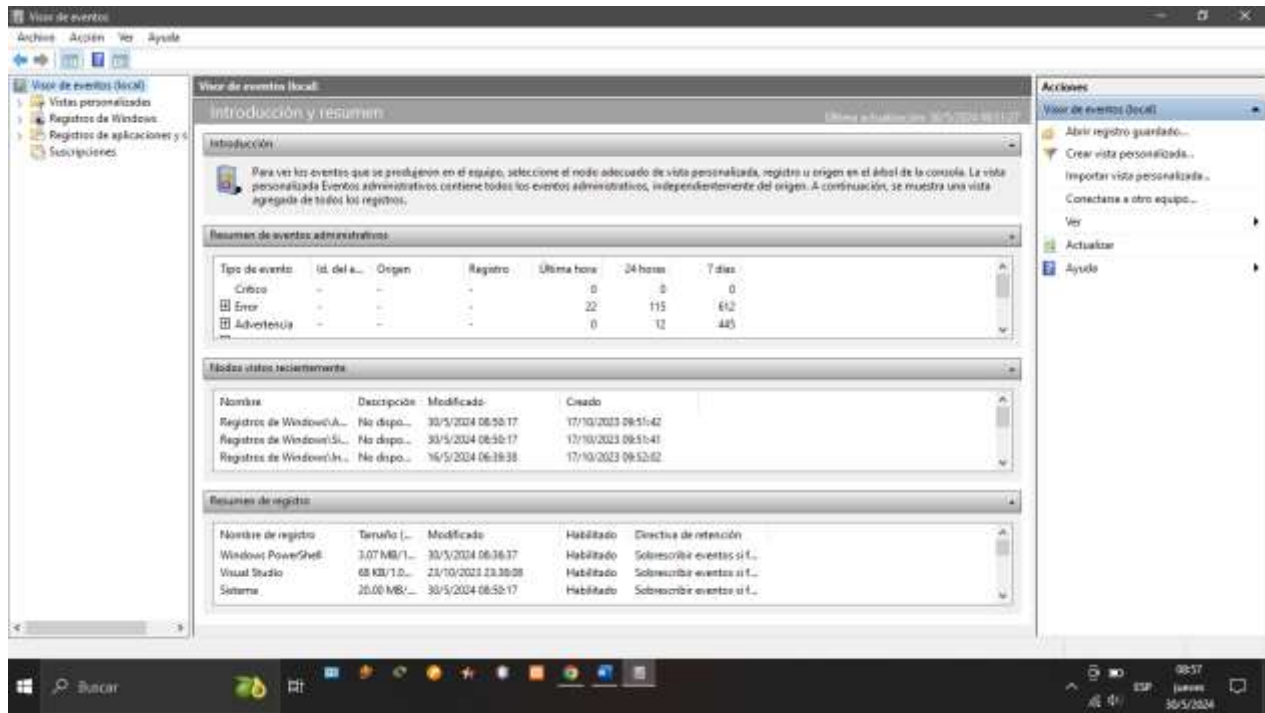
Desarrollo.

Etapas 3 – Auditorias y Bitácoras

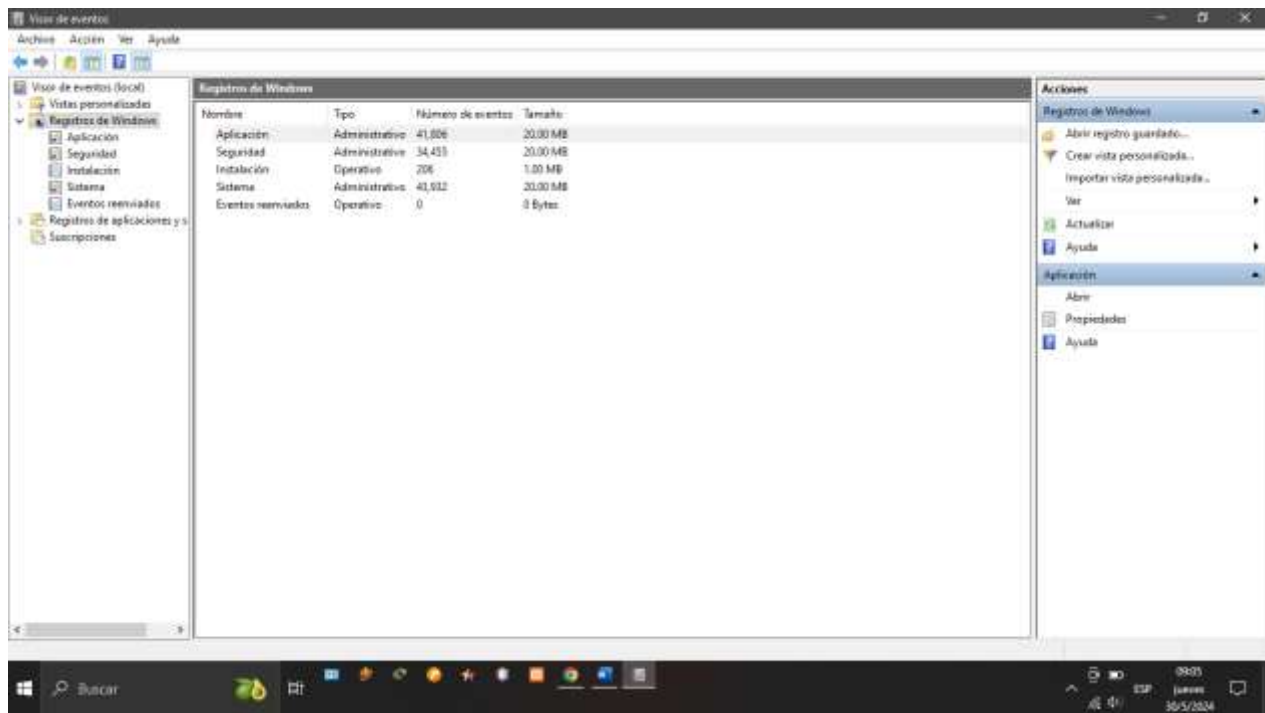


Ingresamos al panel de control y se selecciona Herramientas administrativas

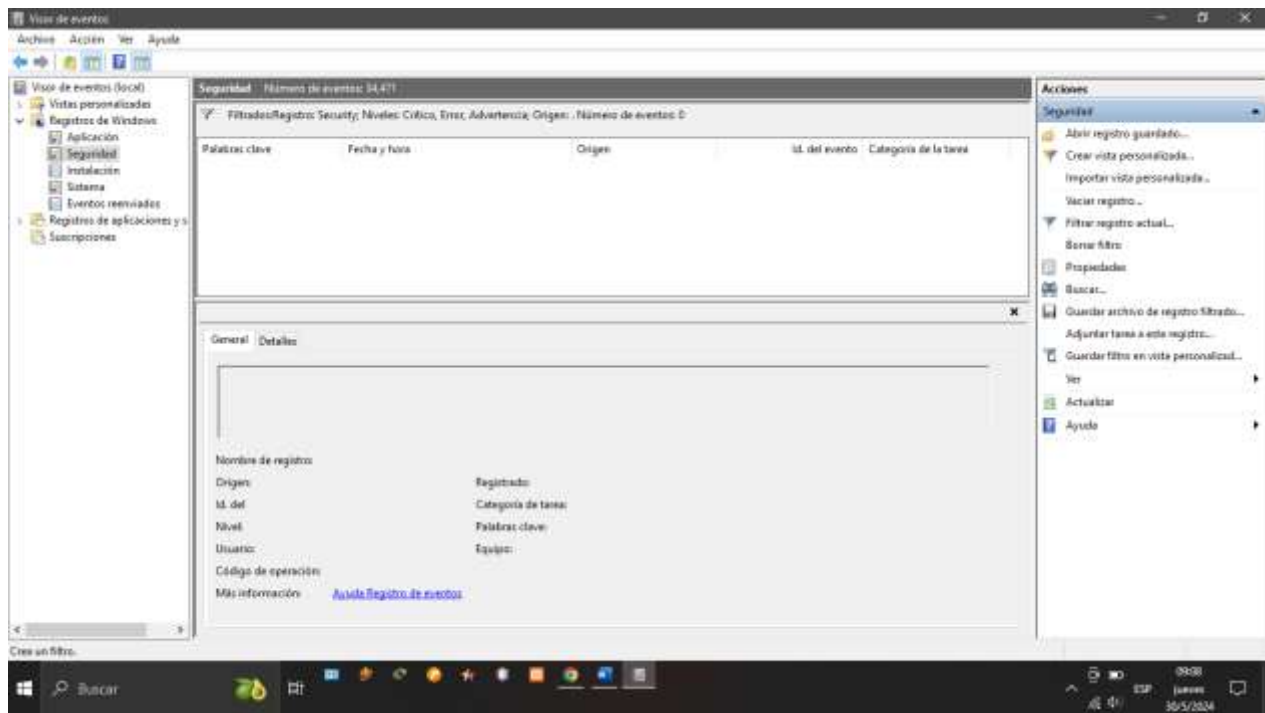




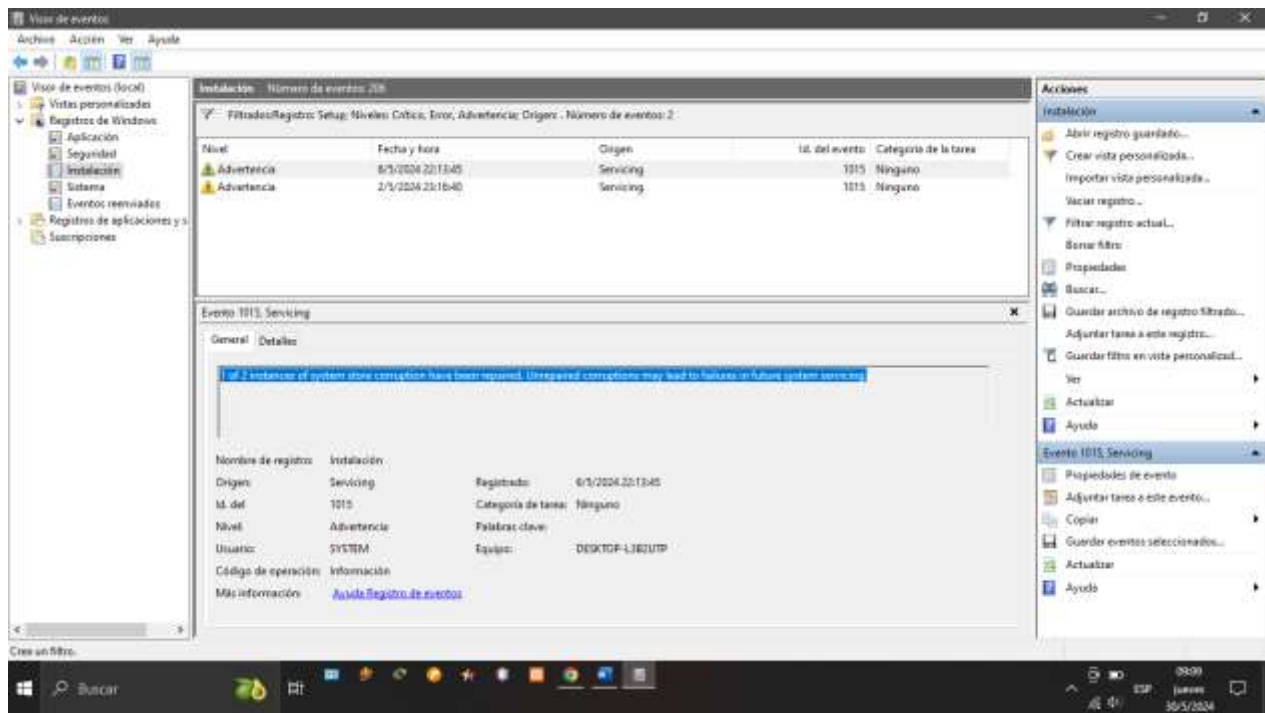
En el visor de eventos podemos visualizar los eventos para auditar el status del equipo



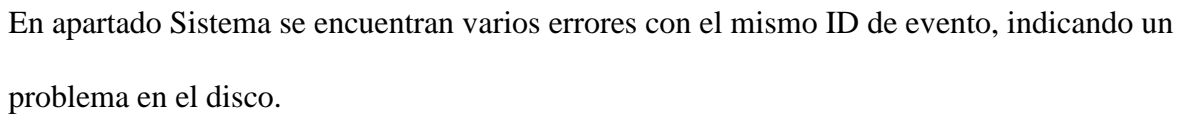
Ingresamos en el apartado de registros de Windows

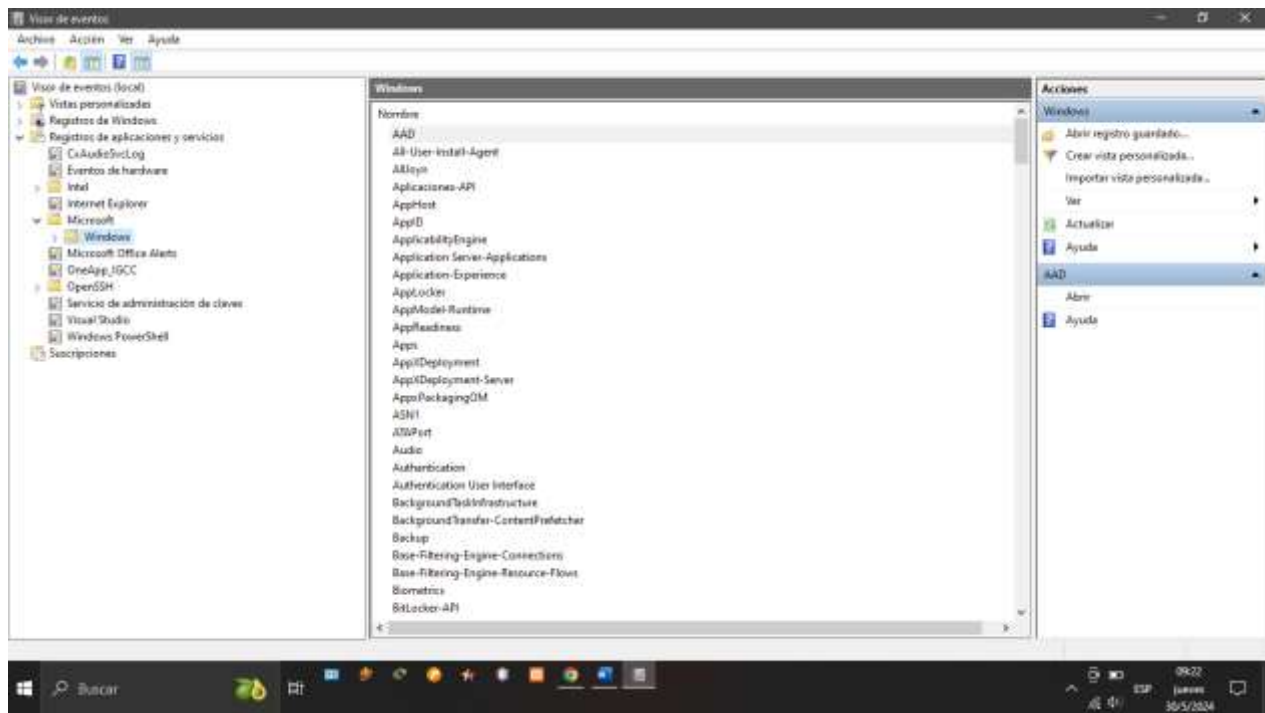


Sin encontrar ningún evento en el apartado de seguridad

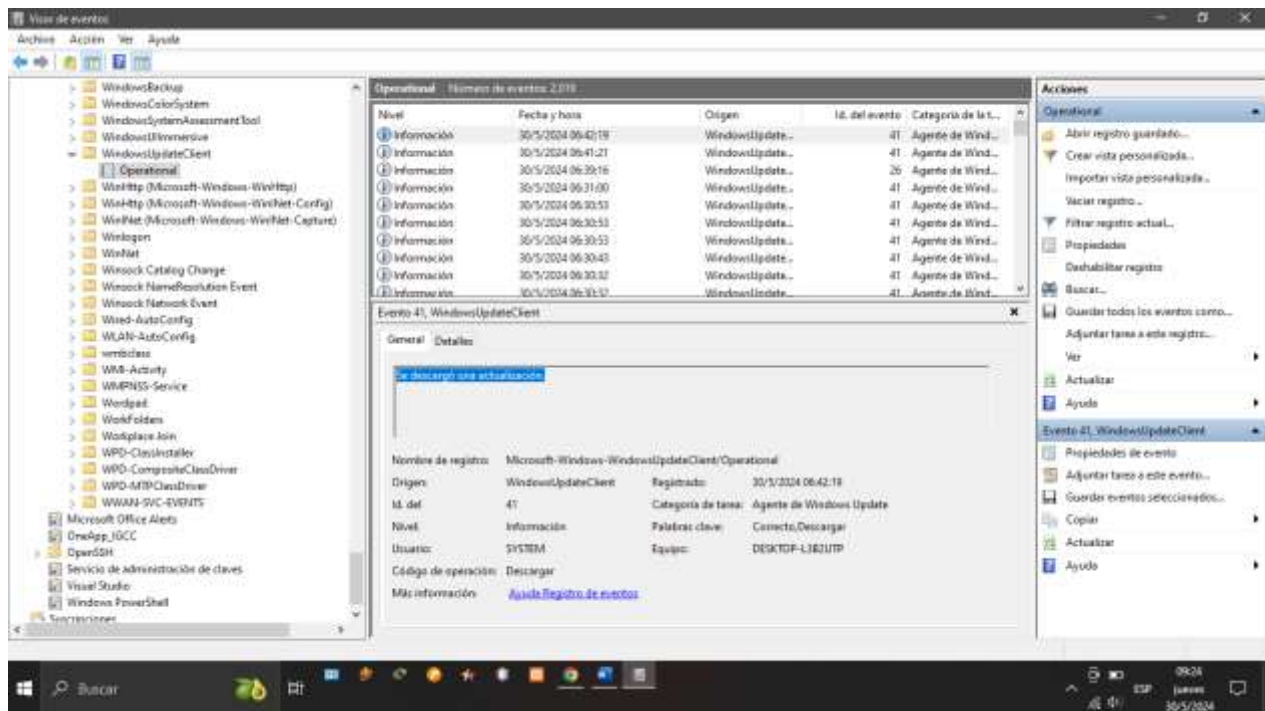


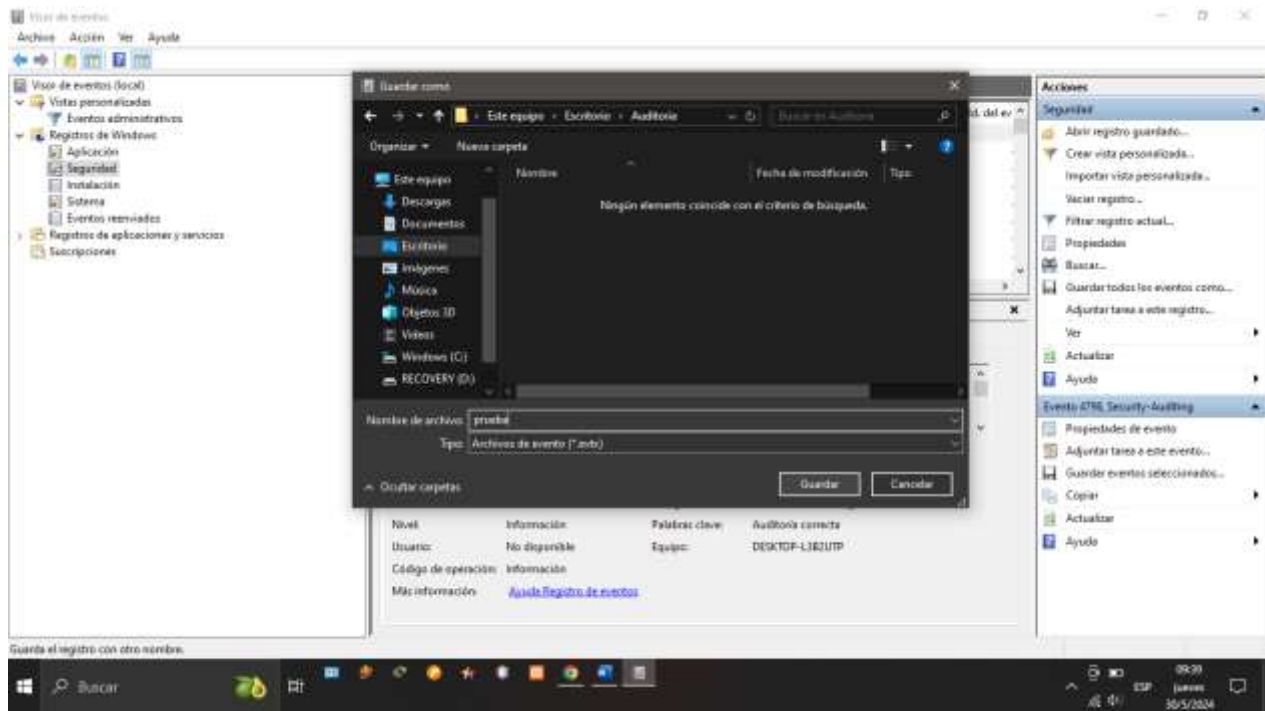
En el apartado de instalación se encontraron 2 advertencias indicando que fueron reparadas



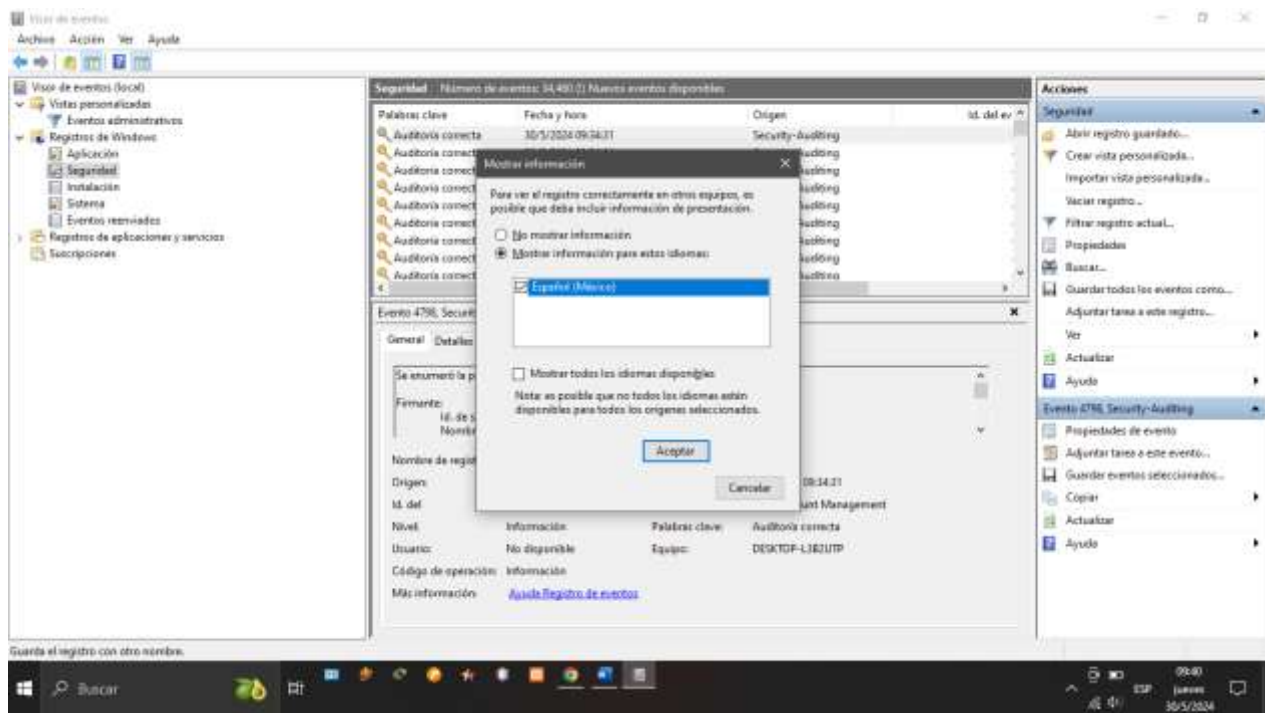


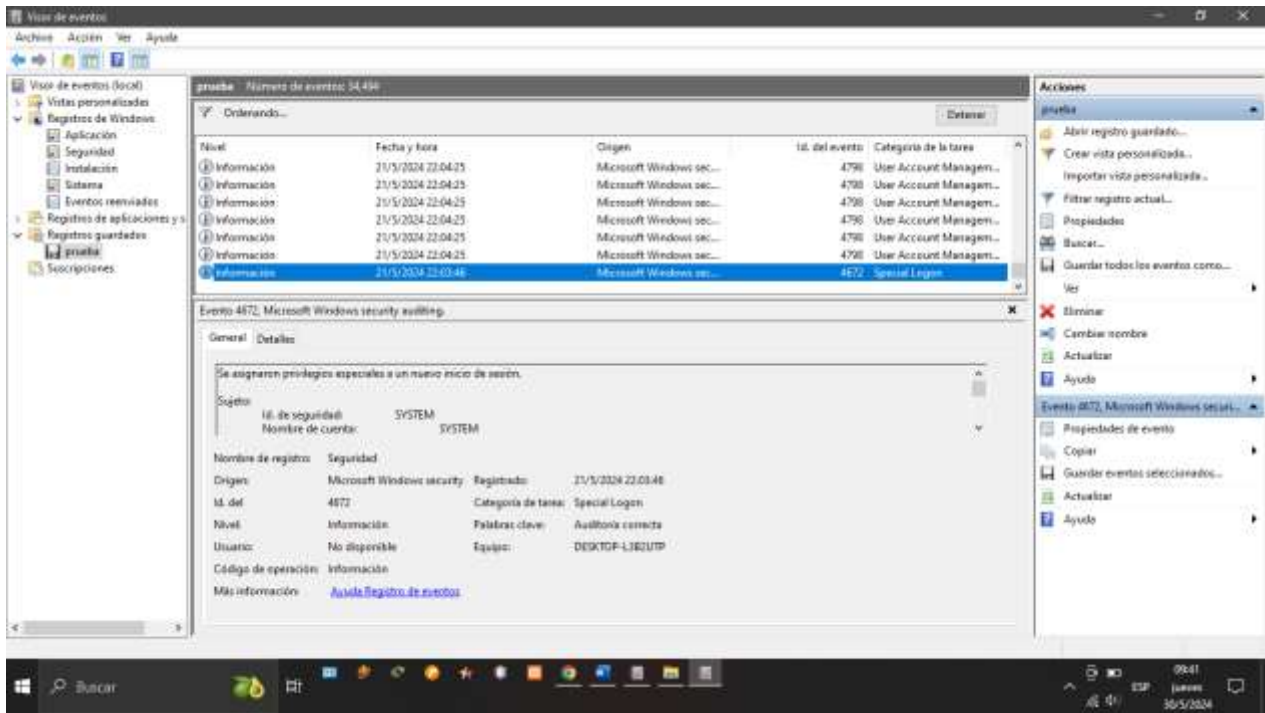
Verificamos el estado de operatividad de Windows update





Y se guarda el evento para futuras consultas





Conclusión.

En resumen, la detección y prevención de ataques de acceso son fundamentales para mantener la seguridad y la integridad de los sistemas y datos para evitar pérdidas monetarias significativas y de credibilidad ante los consumidores, este tipo de prácticas no solo protegen contra pérdidas financieras y de reputación, sino que también aseguran el cumplimiento normativo, manteniendo la confianza de los clientes y socios comerciales, que para mantener y mejorar la seguridad es esencial llevar a cabo las auditorias para poder identificar vulnerabilidades, asegurando el cumplimiento normativo, fomentando la mejora continua facilitando la investigación de incidencias y por medio de las bitácoras se cuenta con un registro detallado de las actividades del sistema, que con las auditorias y bitácoras se forma una base solida para una estrategia de seguridad informática robusta y efectiva.


¿Qué aprendo?

Que mediante este tipo de practica se puede mantener la integridad de la red y los equipos dentro la misma, monitoreando de forma continua cada posible fallo permitiendo reaccionar con anticipación a cualquier posible intrusión, ataque, o mala configuración, asegurando el uso por parte de todos los usuarios, que el monitoreo de red es una practica esencial para garantizar la operatividad, seguridad y eficiencia de las infraestructuras informáticas, proporcionando a los administradores las herramientas necesarias para mantener y optimizar el rendimiento de la red, cumpliendo con la normatividad establecida, y que es un área de oportunidad que me gustaría explorar para poder especializarme y obtener una oportunidad dentro del ámbito laboral de la seguridad de sistemas y redes.

Enlace Github: <https://github.com/Chifer888/Seguridad-informatica-2.git>

Referencias

ChatGPT. (n.d.). <https://chatgpt.com/c/47f50800-efab-4d30-81ef-13f132e0f2e6>

Contando Bits. (2024, January 9). *Como Instalar y Usar Nessus en Windows 10*  [Tutorial Escaneo de Vulnerabilidades] [Video]. YouTube. <https://www.youtube.com/watch?v=-8l2Hqp-eRo>

Global, A. (2024, May 18). *Video 2 Auditoría de Vulnerabilidades en la Red con Nessus* [Video]. Vimeo. <https://vimeo.com/660530360/ad1982a98c>

ChatGPT. (n.d.). <https://chatgpt.com/c/8855ea2e-7f4a-4b98-808b-2758891a1b52>

ChatGPT. (n.d.). <https://chatgpt.com/c/e59e4e7d-9149-45ab-9994-85146dc8dcb3>

Markdefalco. (n.d.). *Visor de eventos* [Video]. Microsoft Learn. <https://learn.microsoft.com/es-es/shows/inside/event-viewer>

