**Paso 5: Operando un Sistema Operativo**

Jesus Augusto Chacón Corredor

Gustavo Jabier Barrio Polo

Luis Carlos Segundo Fonseca Gámez

Ángel David Herrera Vergara

Adriana del Pilar Parra Altahona

Universidad Nacional Abierta y a Distancia (UNAD)  
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Sistemas Operativos  
Código: 202016895A

Tutor(a) a cargo  
Pablo Cesar Monroy Marín

Grupo: 9

Santa Marta, Magdalena  
9 de Diciembre de 2024

INTRODUCCIÓN

En la actualidad, la seguridad informática se ha convertido en un pilar fundamental para las empresas que buscan proteger sus activos digitales frente a amenazas externas e internas. TelecommunicationsAtHand S.A., dedicada al montaje y mantenimiento de redes, enfrenta el desafío de mitigar las vulnerabilidades detectadas en sus sistemas operativos Windows. Estas vulnerabilidades, producto de sistemas desactualizados y configuraciones inseguras, podrían ser aprovechadas por atacantes para comprometer la seguridad de la información.

En este trabajo se aborda el uso del software Nessus, una herramienta líder en la detección de vulnerabilidades, para identificar, clasificar y solucionar riesgos críticos, potenciales y mixtos en los sistemas de la empresa. A través de un enfoque práctico y estructurado, se explican los pasos necesarios para la descarga e instalación de Nessus, la ejecución de escaneos, la interpretación de resultados y la aplicación de medidas correctivas, incluyendo la detección de puertos abiertos y programas débiles.

El propósito es fortalecer la seguridad de los sistemas mediante una solución eficaz que permita no solo resolver los problemas actuales, sino también prevenir futuras amenazas. Este trabajo enfatiza la importancia de mantener una infraestructura tecnológica segura y actualizada, garantizando la protección de la información y la continuidad operativa de TelecommunicationsAtHand S.A.

**OBJETIVO GENERAL**

Identificar y resolver vulnerabilidades críticas, potenciales y mixtas en los sistemas operativos Windows de la empresa TelecommunicationsAtHand S.A., utilizando el software Nessus para fortalecer la seguridad de la información y prevenir posibles ataques internos o externos.

**OBJETIVOS ESPECÍFICOS**

* Realizar la descarga, instalación y configuración de Nessus, garantizando su óptimo funcionamiento para escanear sistemas Windows.
* Ejecutar escaneos detallados con Nessus para detectar vulnerabilidades como puertos abiertos, configuraciones inseguras y programas débiles.
* Interpretar los resultados obtenidos del análisis, clasificando las vulnerabilidades según su nivel de criticidad (crítico, potencial, mixto e informativo).
* Proponer y aplicar soluciones específicas para mitigar las vulnerabilidades detectadas, siguiendo las recomendaciones del software Nessus.
* Establecer un protocolo de monitoreo continuo para prevenir la reaparición de riesgos y fortalecer la protección frente a posibles ataques.

**GUIONES INDIVIDUALES Y VIDEOS**

**Luis Carlos Segundo Fonseca Gámez**

**¿Qué es Nessus?**

es una herramienta de escaneo de vulnerabilidades de red desarrollada por Tenable Network Security. La cual fue creada en 1998 por Renaud Deraison y es una de las soluciones de seguridad más populares y utilizadas en todo el mundo.

**Funcionalidad de Nessus**

* Escaneo de Vulnerabilidades
* Informes Detallados
* Actualizaciones Constantes
* Compatibilidad
* Interfaz Web

**Escaneo de Vulnerabilidades**

Nessus escanea redes, sistemas operativos, aplicaciones y dispositivos de red en busca de vulnerabilidades conocidas y desconocidas. Esto incluye configuraciones erróneas, problemas de seguridad y posibles puntos débiles que podrían ser explotados por atacantes.

**Informes Detallados**

Después de realizar un escaneo, Nessus genera informes detallados que indican las vulnerabilidades encontradas, su nivel de gravedad y recomendaciones para corregirlas.

**Actualizaciones Constantes**

Nessus se actualiza regularmente con nuevas bases de datos de vulnerabilidades para asegurar que siempre esté al día con las amenazas más recientes.

**Compatibilidad**

Es compatible con una amplia variedad de sistemas operativos, incluyendo Windows, Linux y macOS.

**Interfaz Web**

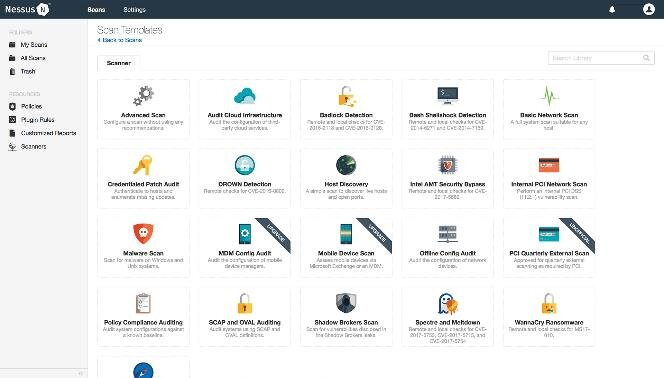


Ilustración 1: Interfaz de Apps en Nessus.

Nessus cuenta con una consola web que permite configurar y gestionar los escaneos, así como visualizar los resultados de manera accesible.

**Nessus**

Nessus es una herramienta fundamental para cualquier organización que busque mejorar su postura de seguridad y proteger su información de posibles amenazas.

Link Video: <https://youtu.be/Xb_KdILxHos>

**Ángel David Herrera Vergara**

**Descarga e instalación de Nessus**

Vamos a explicar el paso a paso de la instalación de Nessus y explorar su uso en un sistema operativo Windows:

1. En primer lugar, nos vamos a página oficial de Nessus por el siguiente link.<https://www.tenable.com/downloads/nessus>
2. En segundo lugar, nos envía a la página oficial y elegimos la mejor opción, según nuestra arquitectura y sistema operativo que estemos usando. Luego le damos en descargar, aceptamos las licencias y elegimos.

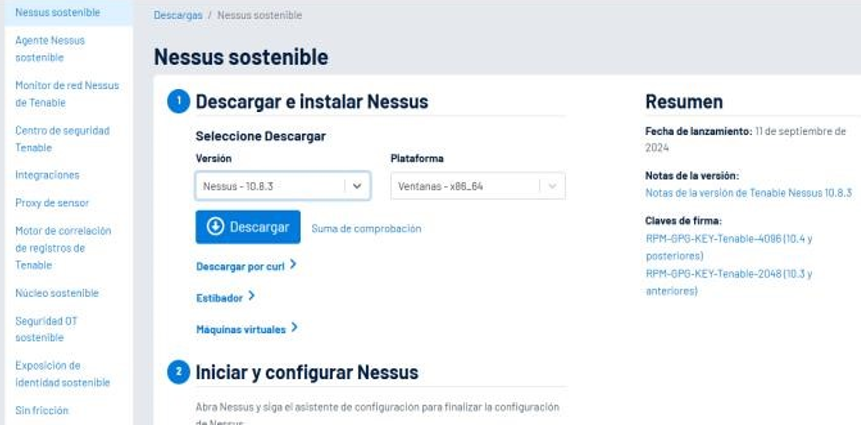
****

Ilustración 2: Descarga del Software Tenable Nessus.

Una vez descargado, ejecutamos el programa de instalación. Luego le damos clic en next, después aceptamos los términos y condiciones y elegimos la ruta que queramos e instalamos el programa.

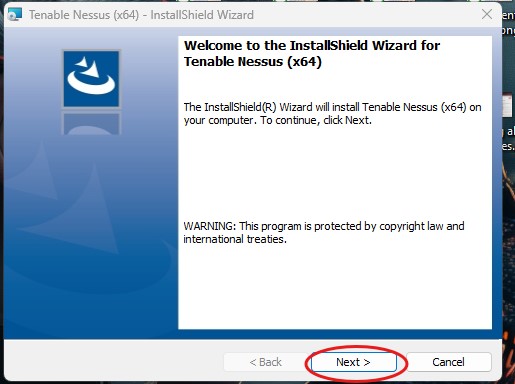


Ilustración 3: Guía de instalación 1.

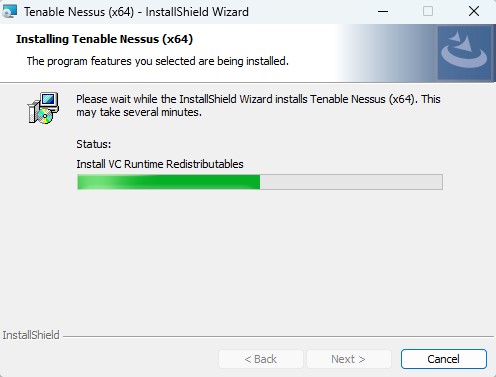


Ilustración 4: Guía de instalación 2.

1. Una vez instalado, le damos en finish, automáticamente nos va a abrir una pestaña y vemos que en el local Host en el puerto 8834, vemos que nos aparece lo que viene a ser la interfaz gráfica de Nessus. le vamos a dar a conectar y nos pedirá registro.

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

Ilustración 5: Portal de Nessus.

1. Ahora nos pide que nos registremos, pero no le daremos en registrar offline, si no en continuar, ya que si lo hacemos nos va a decir que pongamos una licencia; por lo que mejor, le daremos en continuar.

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

Ilustración 6: Configuraciones pre-registro.

1. Nos registramos con nuestros datos

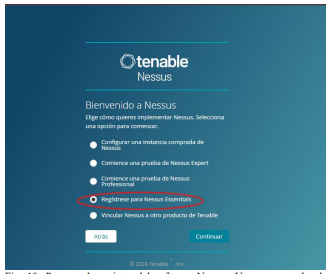


Ilustración 7: Selección de tipo producto a usar de Nessus.

1. Proceso de registro del software Nessus. Una vez completado comenzara la descarga de los pluggins con los que funciona la herramienta.

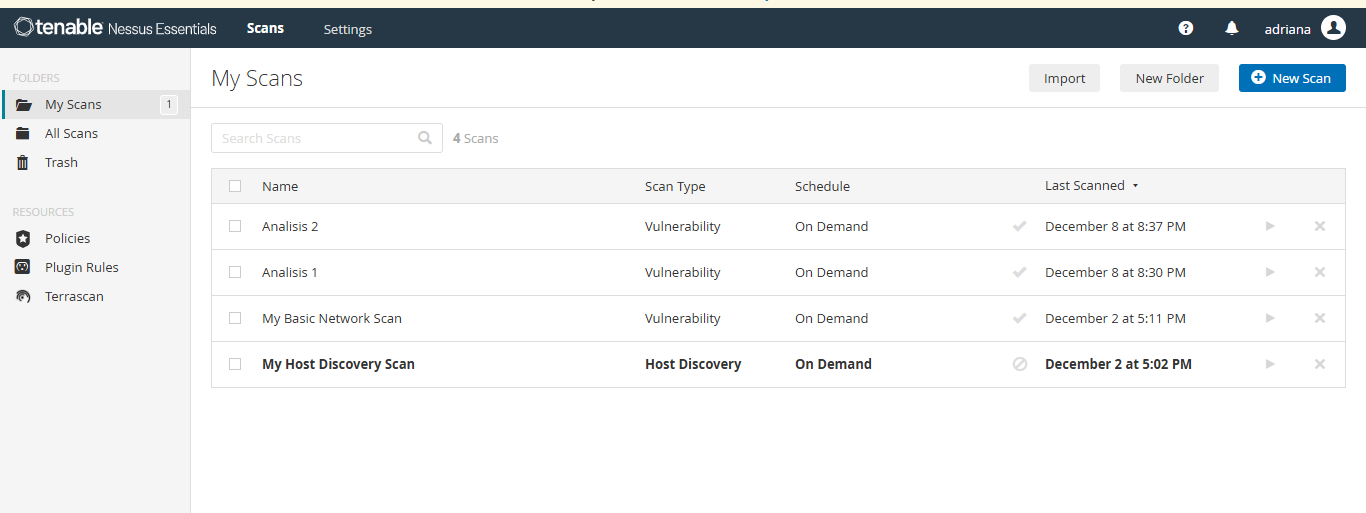
Enlace del video: <https://youtu.be/fjBJ1J2mLhQ>

**Adriana del Pilas Parra Altahona**

**Escaneo de Windows Con La Herramienta de Nessus**

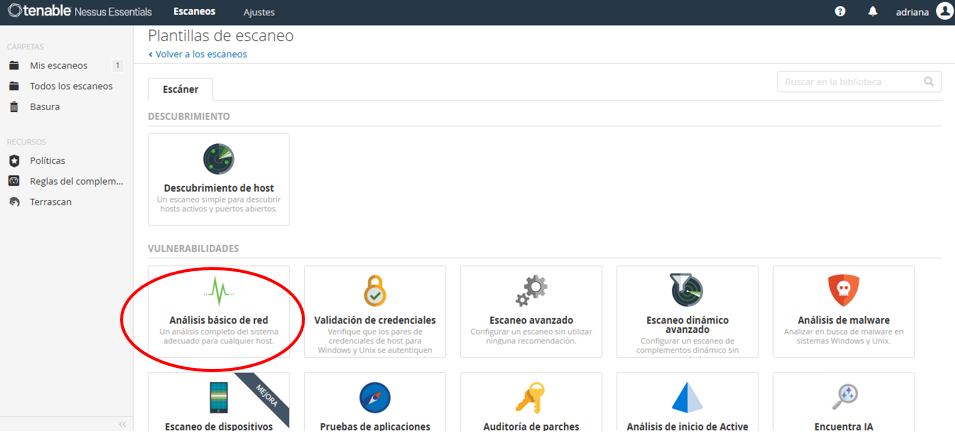
Luego de haber instalado Nessus debemos abrirlo en línea, una vez abierta la herramienta de Nessus procedemos hacer el escaneo de Windows.

1. Estando en la herramienta de Nessus Lo primero que debemos hacer es darle clic en Nuevo Escaneo.

Ilustración 8: Inicio de escaneo con Nessus****

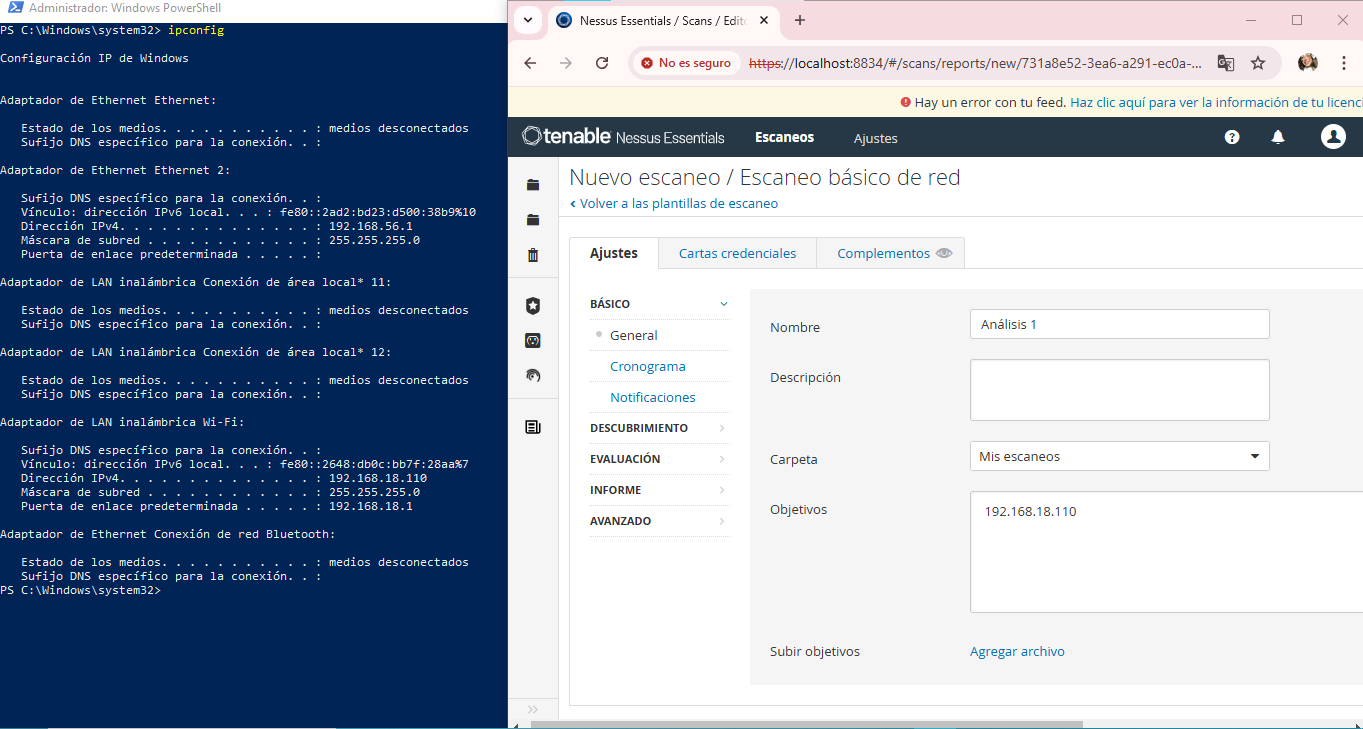
1. En segundo lugar nos van aparecer varias herramientas y haremos un escaneo básico para el Análisis de la red.

Ilustración 9: Menú de Nessus con diferentes herramientas.



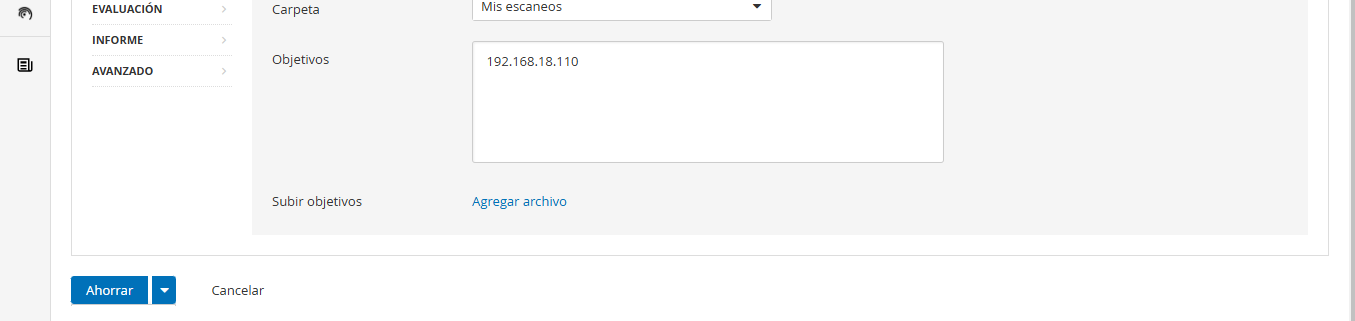
1. Luego nos pide que llenemos las credenciales, colocándole un nombre, la dirección de la careta donde deseamos guardar el escaneo y los objetivos en el cual nos pide colocar la dirección ip de la red del dispositivo, buscamos la ip en el **CMD** de Windows la copiamos y la pegamos en el apartado de los objetivos.

Ilustración 10: En el apartado donde nos pide la dirección ip podemos hallar nuestra del dispositivo en el CMD de Windows, luego hacemos en escaneo básico de la red.



1. Después de haber pegado la dirección ip nos desplazamos hacia abajo y le damos en ahorrar para guardar y comenzar el escaneo.

Ilustración 11: Guardar.



1. Luego encontramos guardado el escaneo en mis escaneos le damos clic en el análisis que estamos haciendo para abrirlo, luego le damos en lanzamiento para así poder proceder con el escaneo.

Ilustración 12: Mis escaneos.

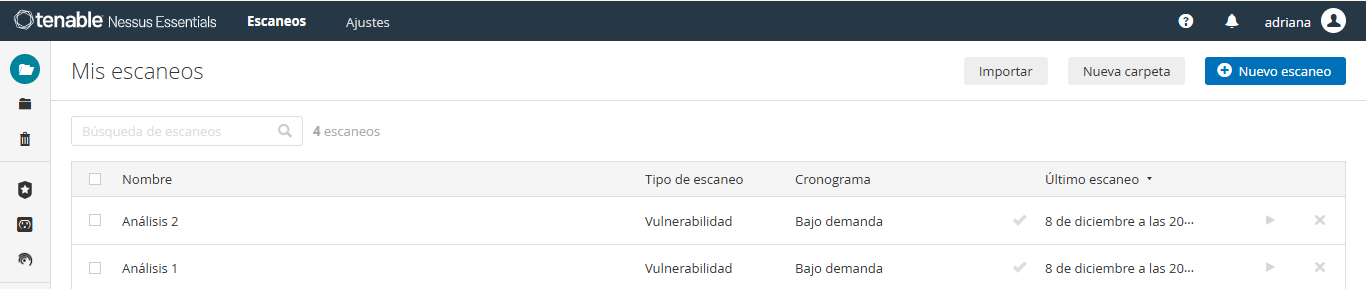
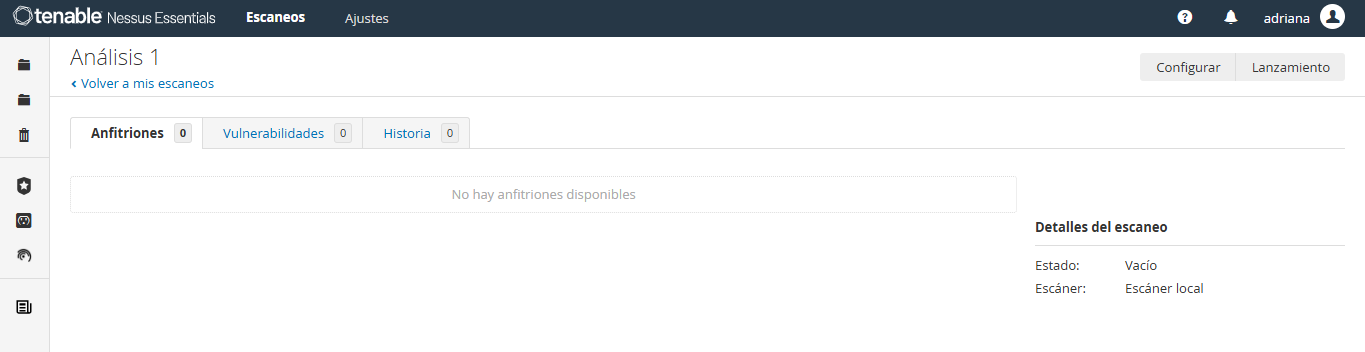


Ilustración 13: Lanzamiento del escaneo para que comience.



1. Luego de haber terminado en escaneo nos van aparecer los resultados generales y de las vulnerabilidades del análisis.

Ilustración 14: Resultados generales.

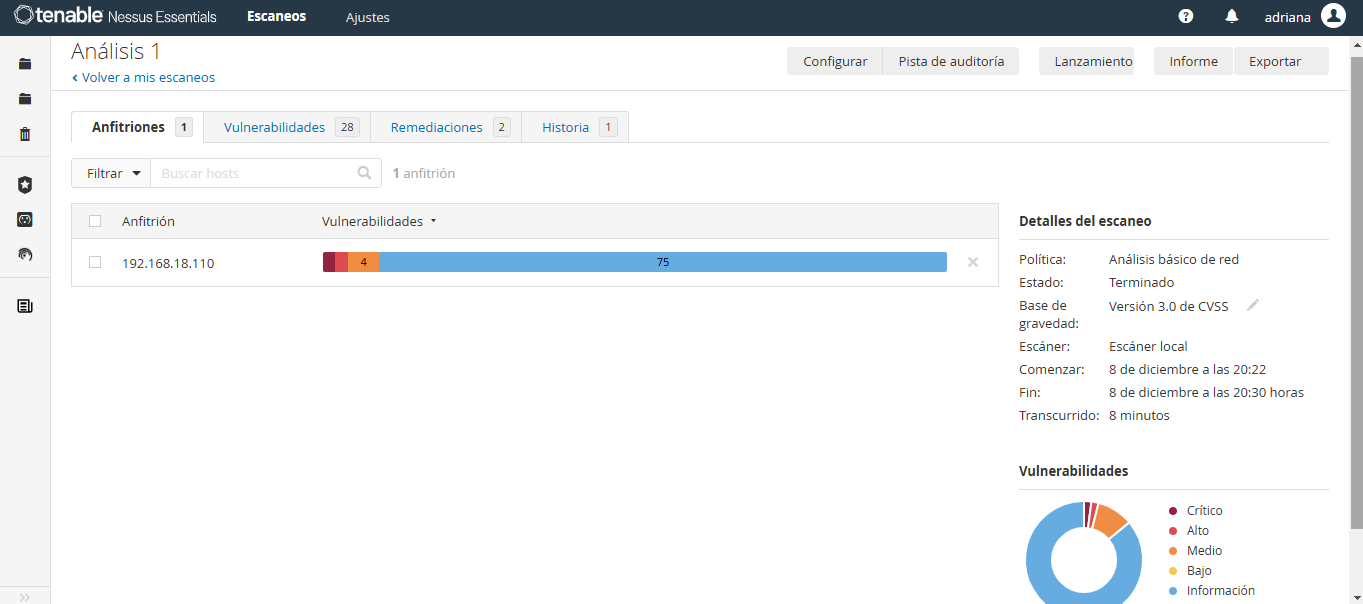
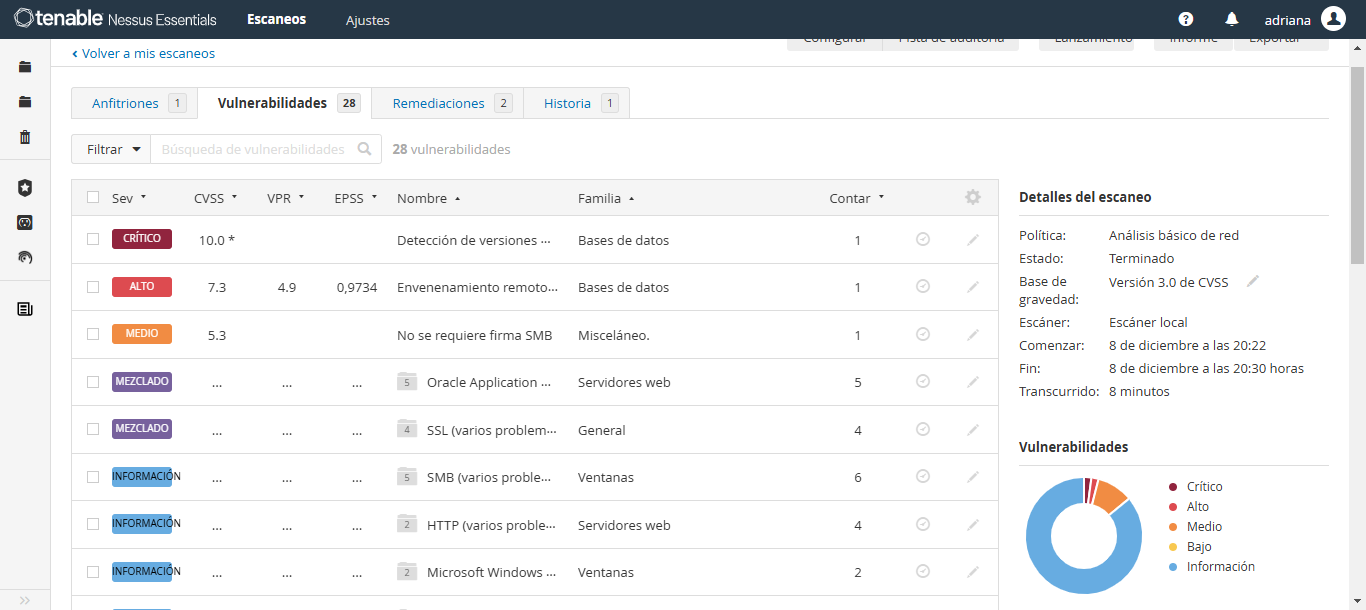
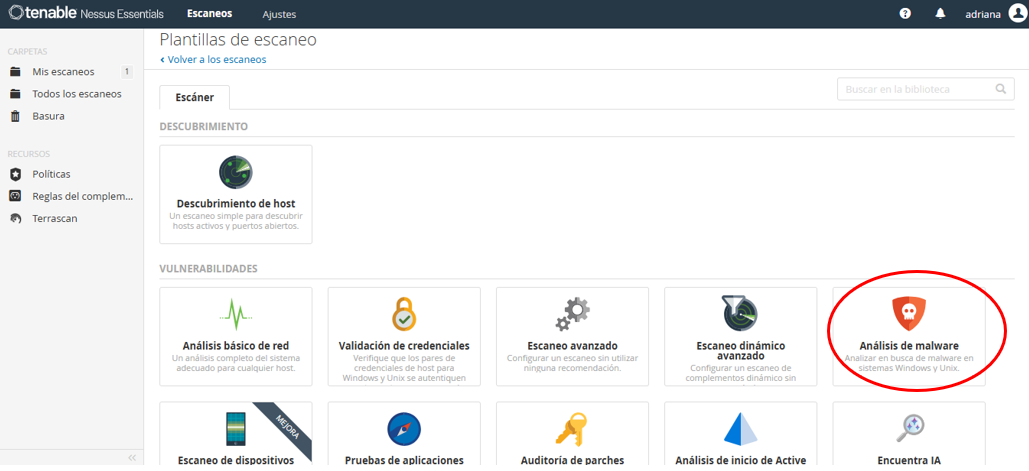


Ilustración 15: Resultado detallado del análisis.



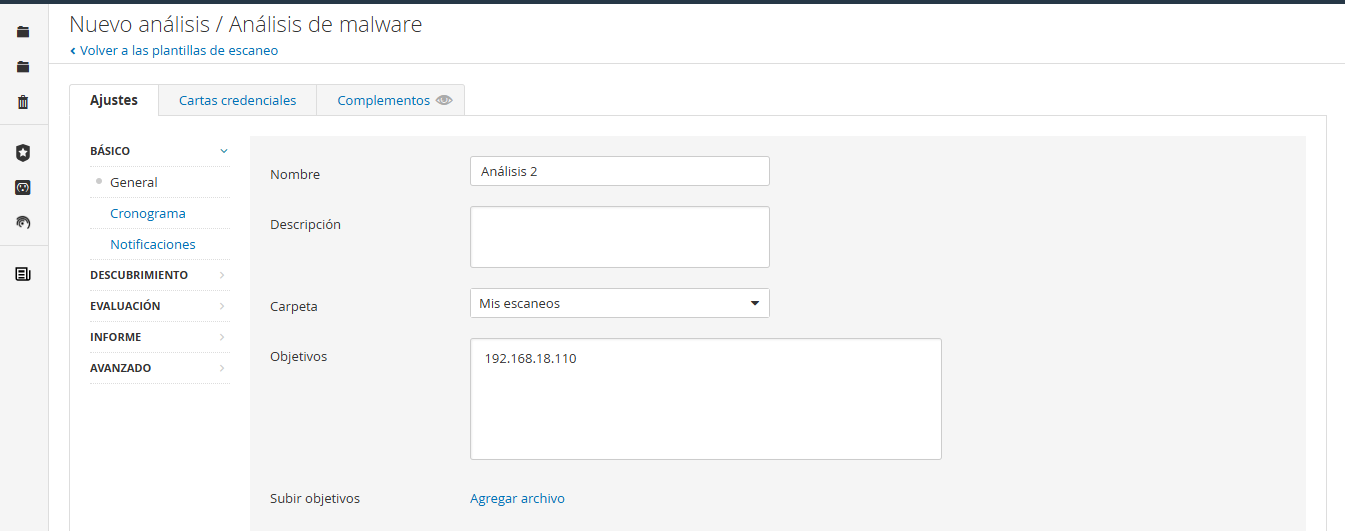
1. Segundo escaneo: Ahora vamos a hacer otro escaneo para ello en primer lugar nos vamos al menú de las herramientas y escogemos la que dice análisis de malware.

Ilustración 16: Ejecutar análisis de malware.



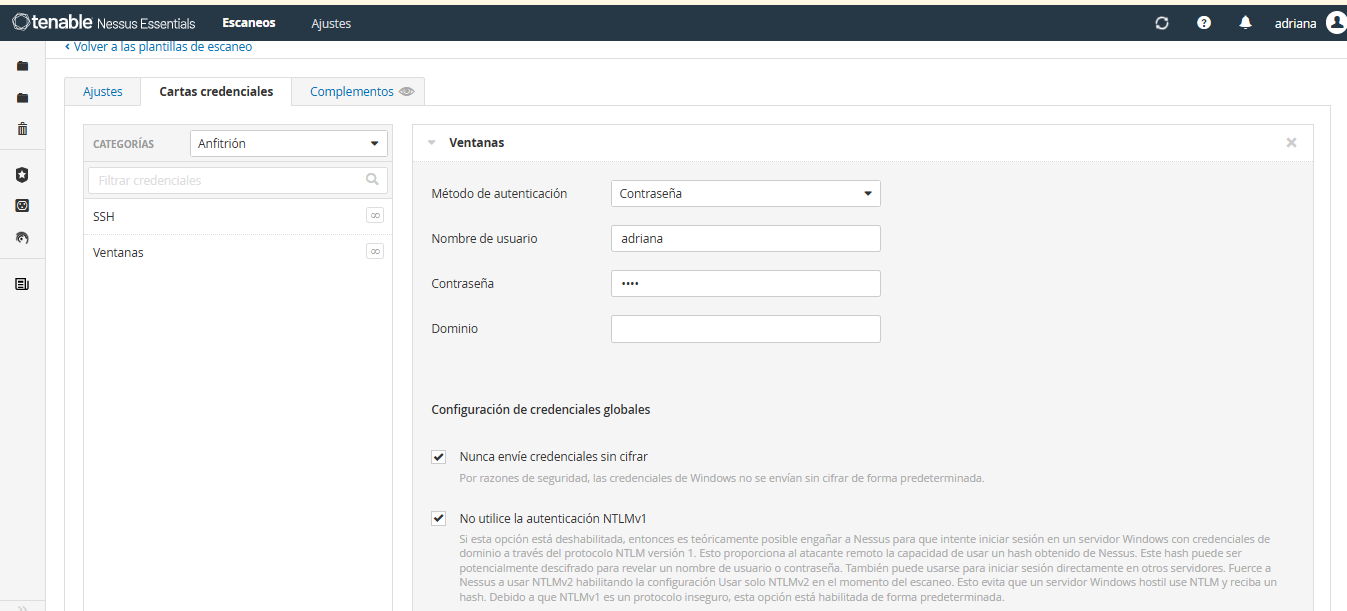
1. En segundo lugar, debemos llenar los campos con las información que se requiere.

Ilustración 17: Rellenar la información básica para hacer el análisis.



1. Tercer lugar, vamos a llenar las credenciales con el nuestro nombre de usuario y la contraseña que utilizamos en la herramienta de Nessus.

Ilustración 18: Credenciales para poder ejecutar el análisis.



1. Para finalizar, lanzamos el análisis y esperamos a que termine, para luego mostrarnos lo encontrado.

Ilustración 19: Lanzamiento del análisis

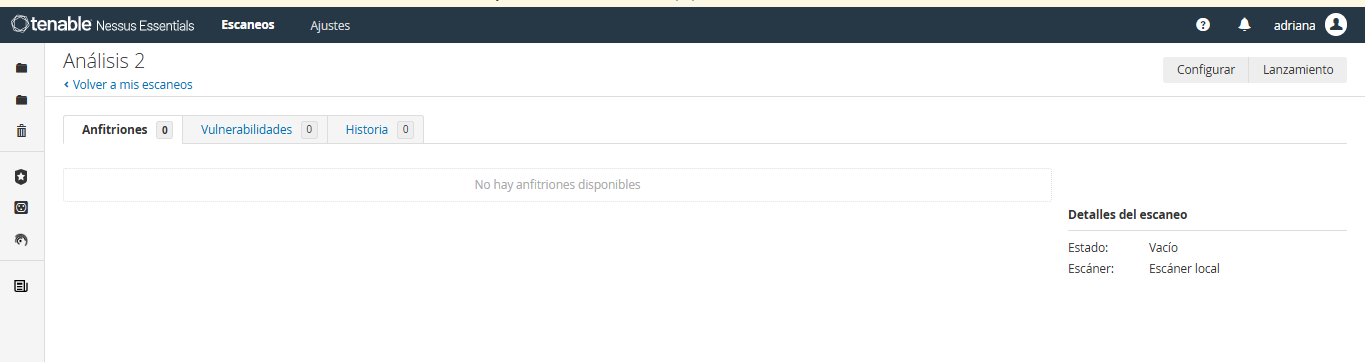


Ilustración 20: Resultados Generales del análisis.

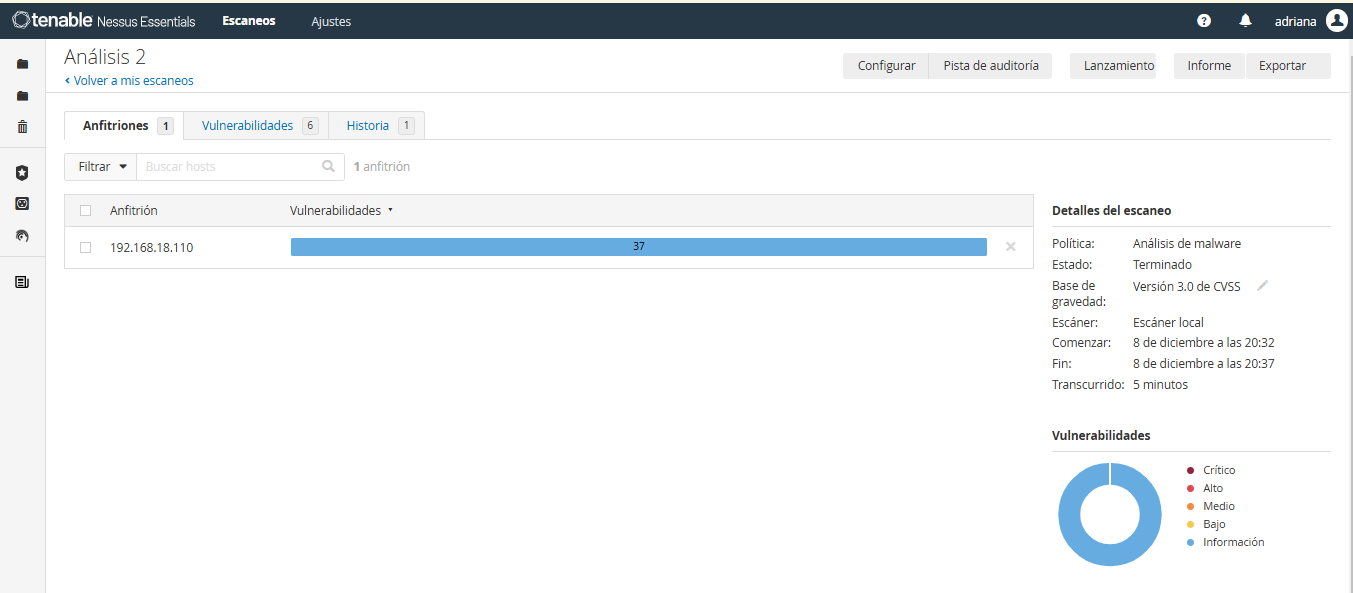
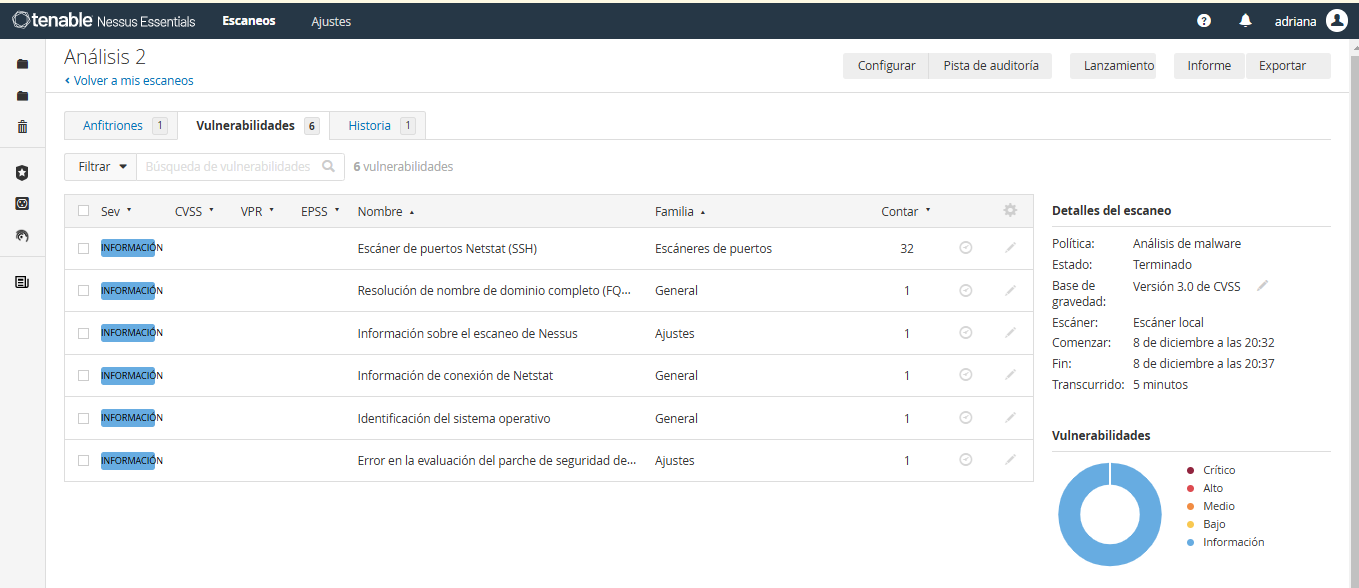


Ilustración 21: Resultados detallados del análisis.



Explicación breve de que significa cada una de las vulnerabilidades:

**Estado crítico:** podemos encontrar las vulnerabilidades que representan un riesgo inmediato el cual debemos solucionar, generalmente estas fallas permiten acceso total o comprometen completamente el sistema.

**Ejemplo:**

* Vulnerabilidades explotables de manera remota (como RCE, Remote code Executión).
* Servicios expuestos con contraseñas por defecto.
* **Estado Alto:** Son vulnerabilidades con un alto potencial de explotación que podrían permitir a atacantes comprometer la confidencialidad.
* **Estado Medium:** Vulnerabilidades que requieren ciertas condiciones para ser explotadas y tienen un impacto menor.

Link de Video: <https://youtu.be/vG9QjNu_SEQ>

**Jesus Augusto Chacon Corredor**

**Interpretación de resultados**

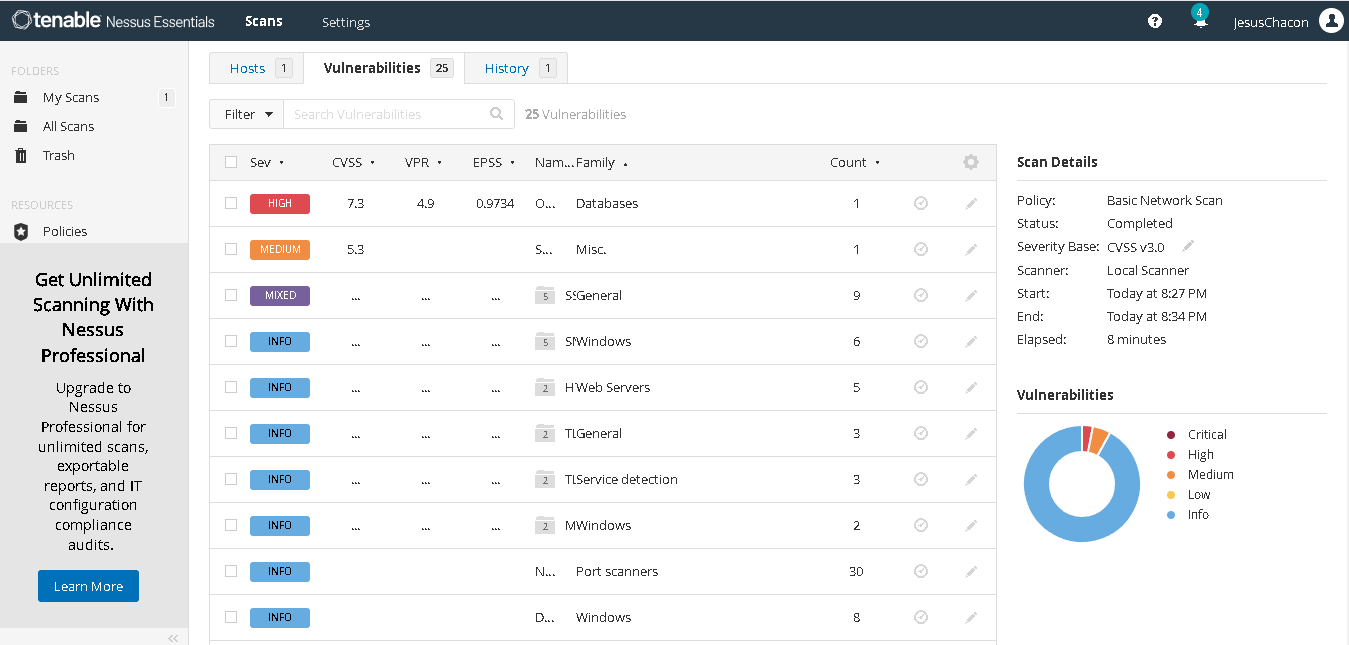
****

Ilustración 22: Resultados de escaneo con Nessus.

**Gráfica de Vulnerabilidades**

Distribución por severidad: Muestra un desglose en forma de gráfico circular con las categorías Critical, High, Medium y Low, lo que ayuda a visualizar la proporción de problemas críticos frente a otros menos graves.

En el programa Nessus, mi interpretación de los resultados se centra en identificar vulnerabilidades detectadas en el análisis. Aquí te explico de forma clara cómo interpretar lo que muestra la imagen del escaneo de mi dirección IP en la siguiente lista de vulnerabilidades:

**Lista de Vulnerabilidades:**

**High (Alta):**

Vulnerabilidades peligrosas, pero no tan críticas como las anteriores porque pueden requerir acceso específico o conocimientos técnicos avanzados para ser explotadas.

**Ejemplo:**

* Un servicio expuesto con credenciales débiles pero no por defecto, como un servidor SSH con contraseña fácil de adivinar.

****

Ilustración 23: Nivel alto de vulnerabilidad detectado.

**Medium (Media Severidad):**

Estas vulnerabilidades no representan un riesgo inmediato, pero pueden ser explotadas si se combinan con otras fallas o si el atacante tiene acceso a más información del sistema.

**Ejemplo:**

* Un software con una versión desactualizada, pero que no tiene un exploit público conocido.
* Falta de cifrado en conexiones internas.

****

Ilustración 24: Nivel medio de vulnerabilidad detectado.

**Mixed (Mixta):**

Estas aparecen cuando Nessus detecta una mezcla de vulnerabilidades de diferentes niveles de severidad en un mismo host o sistema.

**Ejemplo:** Un servidor con vulnerabilidades críticas y bajas detectadas al mismo tiempo.

****

Ilustración 25: Nivel mixto de vulnerabilidad detectado.

**Info (Informativas):**

No son vulnerabilidades propiamente dichas, sino información que Nessus detecta y considera relevante para mejorar la seguridad.

**Ejemplo:**

* Detección de un servicio o puerto abierto que podría ser mal utilizado.
* Versiones de software instaladas (sin vulnerabilidad conocida).

****

Ilustración 26: Nivel bajo, información de vulnerabilidad detectado.

Tipo de Vulnerabilidad: Puede ser "Exploitable", "Misconfiguration", etc., indicando el tipo de riesgo, las cuales son:

**Exploitable (Explotable):**

Se refiere a vulnerabilidades que **pueden ser aprovechadas directamente por un atacante** para comprometer un sistema.

**Ejemplo:**

Una falla en el código de un software que permite que un atacante ejecute comandos maliciosos en tu servidor.

**¿Qué hacer?**

* Actualizar el software afectado o aplicar parches de seguridad.
* Implementar controles adicionales, como un firewall, para mitigar el riesgo.

**Misconfiguration (Mala configuración):**

Esto ocurre cuando un sistema, aplicación o dispositivo **está configurado de manera incorrecta o insegura**, lo que deja puertas abiertas para ataques.

**Ejemplo:**

* Usar contraseñas débiles o por defecto.
* Tener permisos excesivos en carpetas o usuarios.
* Exponer puertos innecesarios a internet.

**¿Qué hacer?**

* Revisar y ajustar configuraciones siguiendo las mejores prácticas de seguridad.
* Deshabilitar servicios o funciones que no sean necesarias.

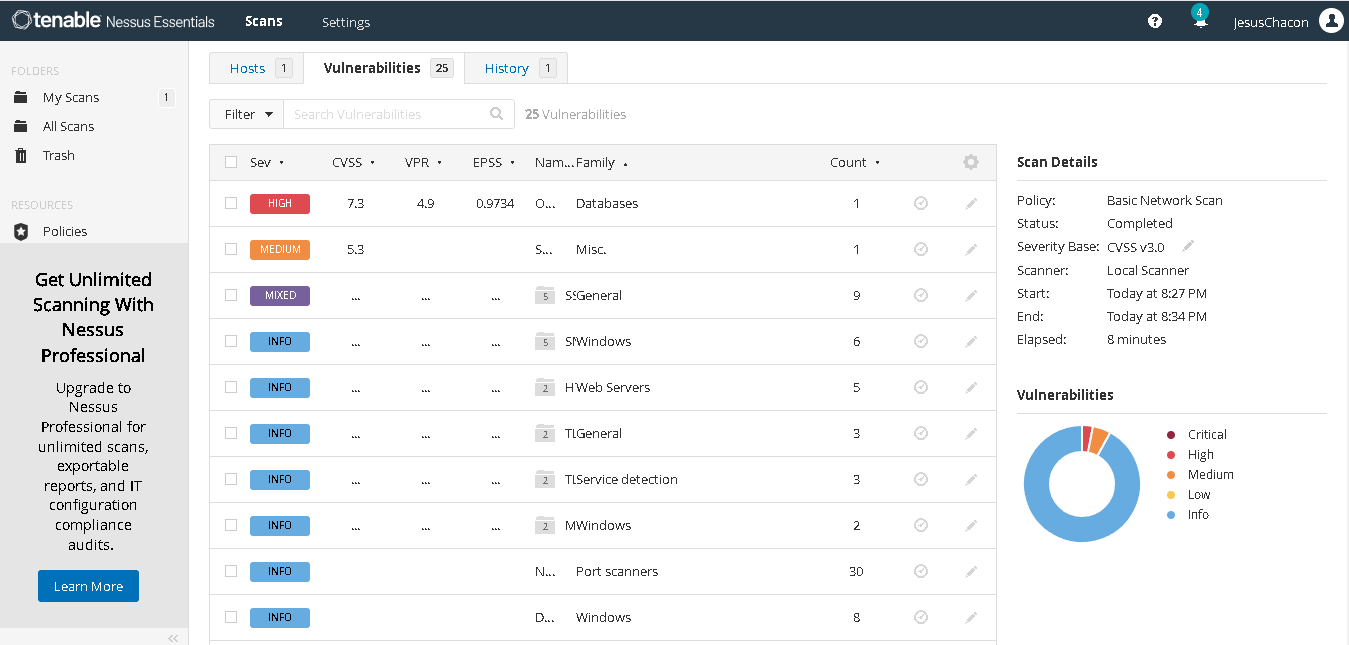
****

Ilustración 27: Vulnerabilidades encontradas.

**Detalles del Escaneo en mi computadora:**

* Host Escaneados: Indica cuántos dispositivos fueron analizados.
* Estado del Escaneo: Muestra si el análisis fue completado o está en progreso.
* Tiempo del Escaneo: Cuánto tardó el proceso en realizarse.
* Cantidad Total de Vulnerabilidades: Suma todos los problemas detectados.

*Link Video:*<https://youtu.be/M9V_auWSn5o>

**Gustavo Jabier Barrios Polo**

**Como solucionar los problemas encontrados con la herramienta Nessus.**

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

Ilustración 28: Pantalla principal de escaneo con Nessus.

Después de un análisis básico en la herramienta Nessus se han identificado 21 vulnerabilidades donde 2 de las 21 son de tipo medio y las otras son de información; Las vulnerabilidades de nivel medio identificadas representan riesgos importantes para la seguridad de la red, ya que, aunque no son críticas, pueden ser explotadas fácilmente si no se toman las medidas adecuadas.



Ilustración 29: Descripción de vulnerabilidad media.

Como podemos observar en la imagen, uno de los problemas destacados es la falta de confianza en los certificados SSL. Los certificados SSL son fundamentales para asegurar las conexiones entre clientes y servidores mediante el cifrado de datos y la autenticación de las partes involucradas. Sin embargo, en este caso, se identificó que los certificados no cumplen con los estándares de confianza, lo que puede deberse a varias razones: pueden ser certificados auto firmados (no emitidos por una autoridad de certificación reconocida), estar caducados o utilizar algoritmos de cifrado desactualizados y vulnerables. Estas fallas crean una brecha de seguridad significativa, ya que los datos transmitidos a través de estas conexiones pueden ser interceptados o manipulados. Este tipo de vulnerabilidad facilita ataques donde un atacante intercepta y controla las comunicaciones, accediendo a información sensible como credenciales, datos personales o financieros. Para mitigar este riesgo, es necesario reemplazar los certificados defectuosos por certificados emitidos por una autoridad confiable, asegurarse de que estén actualizados y compatibles con los estándares modernos de seguridad, y configurar correctamente los servidores para evitar errores en la cadena de confianza.

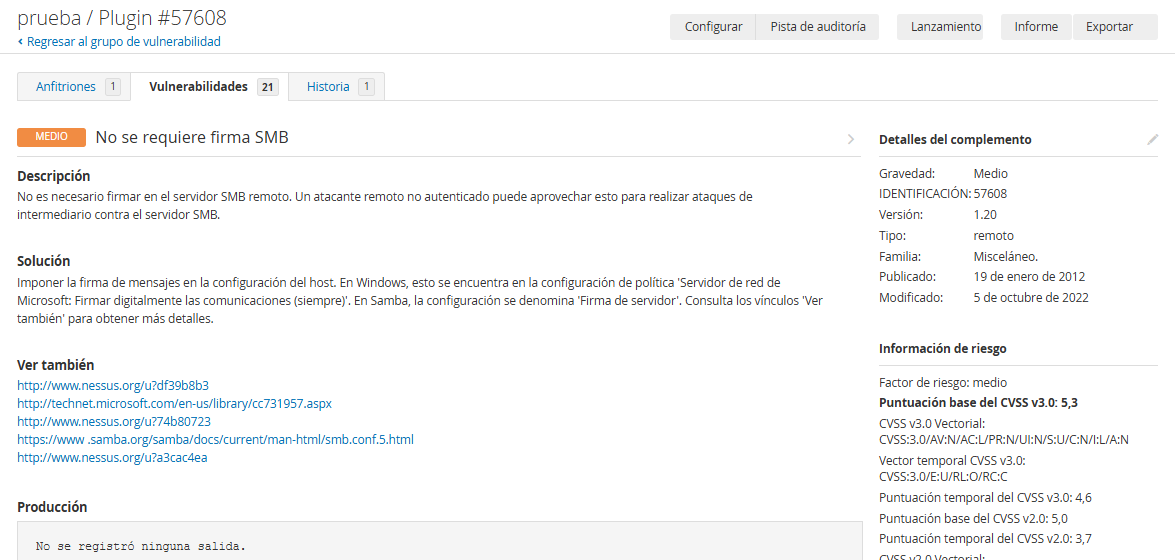


Ilustración 30: información de vulnerabilidad media.

Por otro lado, como podemos observar en el análisis tenemos otro problema crítico identificado que es la configuración insegura del protocolo SMB (Server Message Block), ampliamente utilizado en entornos de Windows para el intercambio de archivos, impresoras y otros recursos compartidos. En este caso, observamos que no se requiere una firma SMB, lo que significa que las comunicaciones entre clientes y servidores no están verificadas ni protegidas contra modificaciones no autorizadas. Esta falta de autenticación en las comunicaciones abre la posibilidad a que un atacante pueda interceptar, alterar o incluso suplantar mensajes entre las partes, permitiendo ataques como la suplantación de identidad o el envío de datos maliciosos. Además, la falta de firma SMB también podría facilitar la propagación de malware o ransomware en la red, ya que no existe una capa de protección que garantice la integridad de los datos en tránsito. Para resolver esta vulnerabilidad, se debe habilitar la opción de firma SMB en las configuraciones del servidor y cliente, asegurando que todas las conexiones sean autenticadas y protegidas con cifrado.

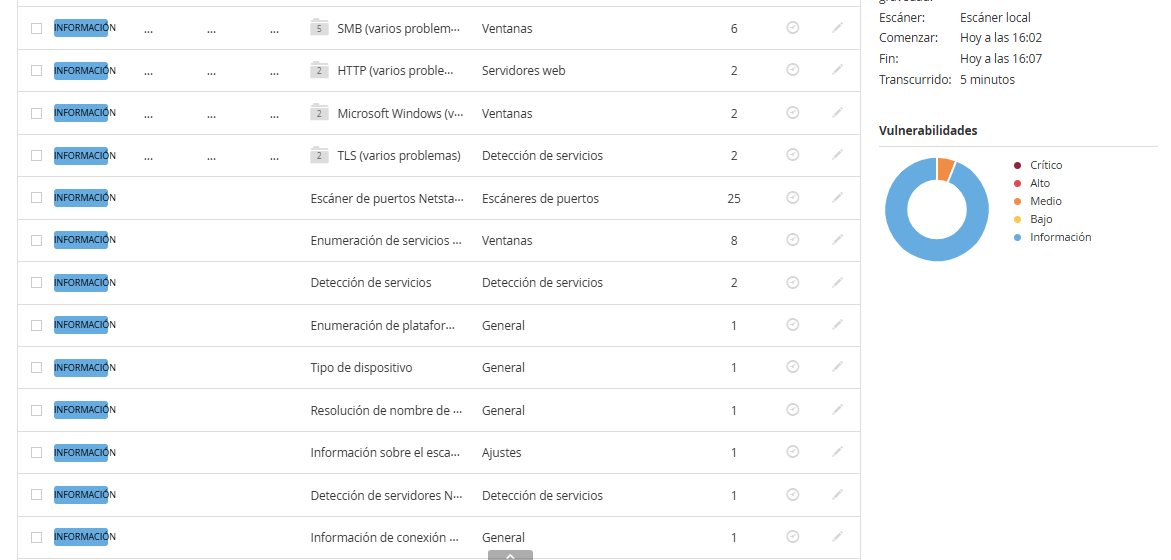


Ilustración 31: Información sobre posibles vulnerabilidades.

Y Por último tenemos, Las vulnerabilidades de nivel "información" las cuales nos indican configuraciones que, aunque no representan un riesgo directo, podrían ser aprovechadas por atacantes si no se gestionan adecuadamente. Por ejemplo, el análisis reveló puertos abiertos como el 135, 137, 138, etc. estos puertos identificados incluyen servicios como NetBIOS, CIFS, DCE/RPC, y Nessus, entre otros, que son vulnerables a ataques de suplantación, malware y acceso no autorizado.

Si estos servicios no están configurados con seguridad adecuada, como certificados válidos o restricciones de acceso, podrían filtrar información sensible. Asimismo, el soporte a versiones obsoletas de TLS, como TLS 1.0 o 1.1, expone conexiones a ataques conocidos. Entonces es recomendable cerrar puertos no utilizados, reforzar los servicios en uso, y actualizar configuraciones para soportar únicamente protocolos y cifrados modernos.

*Link de video individual:* [*https://youtu.be/w1XOm-hG64g*](https://youtu.be/w1XOm-hG64g)

**REQUERIMIENTOS STAKEHOLDERS**

La empresa TelecommunicationsAtHand S.A ofrece en su portafolio de servicios: el montaje y mantenimientos de redes en diferentes topologías y coberturas, provee los insumos necesarios y la mano de obra para los montajes de redes a satisfacción del usuario, para cumplir a cabalidad con los requerimientos en la elección de software con configuraciones y especificaciones concretas. Esta empresa contrató un servicio de auditoría en seguridad informática, la cual arrojó el siguiente requerimiento: “Sistemas operativos no actualizados, lo cual da origen a vulnerabilidades que ponen en riesgo la seguridad de la información”, por lo anterior esta empresa requiere conocer el proceso para auditar sus sistemas operativos Windows y detectar de forma oportuna posibles vulnerabilidades. Para ello requiere una consultoría para dar solución a dicho requerimiento por medio del software Nessus.

Para dar cumplimiento a los requerimientos anteriores, el grupo #9 de ingenieros de la Universidad Abierta y a Distancia, dará solución a la problemática de la empresa TelecommunicationsAtHand por medio del software Nessus, localizando dentro de los sistemas los puntos críticos y vulnerables de los sistemas operativos de cada equipo computo en servicio, solución que veremos en el siguiente video.

Link Video Conferencia de Instalación y Vulnerabilidades de los Sistemas Operativos:

<https://youtu.be/u9vpuItZymE>

En base a la conferencia anterior, pudimos evidenciar, que es el programa Nessus y su funcionalidad, la descarga e instalación de Nessus, escaneo de Windows con la herramienta de Nessus, interpretación de los resultado del escaneo, y la resolución de las vulnerabilidades encontradas. Algunas vulnerabilidades encontradas se registran como riesgos potenciales, críticos, mixtos e informativos, asi como la resolución de los mismos, lo cual como ya se mencionó anteriormente, nos facilita la detección de posibles puertos abierto o programa débiles por los cuales pueda la empresa TelecommunicationsAtHand ser víctima de un atacante externo o interno.

**CONCLUSIÓN**

La seguridad informática es un componente esencial para la sostenibilidad de cualquier organización en el entorno digital actual. A lo largo de este trabajo, se ha demostrado cómo el uso del software Nessus permite identificar, clasificar y resolver vulnerabilidades críticas, potenciales y mixtas en los sistemas operativos Windows, abordando eficazmente los riesgos que amenazan la información sensible de TelecommunicationsAtHand S.A.

Se cumplió con los objetivos planteados al desarrollar un proceso que incluyó la configuración de Nessus, la ejecución de escaneos detallados, la interpretación de resultados y la aplicación de medidas correctivas. Esto permitió evidenciar vulnerabilidades como puertos abiertos y programas inseguros, garantizando una solución inmediata para mitigar estos riesgos. Además, se enfatizó la importancia de establecer un monitoreo continuo como estrategia preventiva para evitar futuras amenazas.

En conclusión, el enfoque presentado no solo resuelve los problemas actuales, sino que establece una base sólida para fortalecer la seguridad tecnológica de la empresa, asegurando su protección frente a posibles ataques internos y externos. Este proceso refleja la necesidad y los beneficios de adoptar políticas de actualización y herramientas avanzadas como Nessus en la gestión de la ciberseguridad.

**REFERENCIAS**

Raya Cabrera, J. L. (2015). [*Implantación de sistemas operativos*](https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/62453?page=209). RA-MA Editorial. (Páginas. 209 - 289). <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/62453?page=209>

Raya Cabrera, J. L. (2015). [*Implantación de sistemas operativos*](https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/62453?page=425). RA-MA Editorial. (Páginas. 425 - 455). <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/62453?page=425>

Carvajal Palomares, F. (2017). [*Instalación y actualización de sistemas operativos Transversal*: UF0852](https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/51111?page=169). Editorial CEP, S.L. (Páginas. 169 - 192). <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/51111?page=169>