

## Actividad | 1 |

Detección y Prevención de Ataques de Acceso

---

### Seguridad Informática II

Ingeniería en Desarrollo de Software



academi**ag**lobal

TUTOR: Jessica Hernández

ALUMNO: Yanira Lizbeth Lopez Navarro

FECHA: 14/01/2024

Índice

Introducción ..... 3

Descripción ..... 4

Justificación ..... 5

Desarrollo: ..... 6

Conclusión ..... 26

Referencias ..... 27

## Introducción

En la era digital actual, donde estamos todos conectados y dependemos en gran medida de nuestros sistemas informáticos, la seguridad se vuelve más vital que nunca. Es por ello que hoy nos toca enfocarnos en temas de protección digital que nos permitan explorar la detección y prevención de ataques de acceso, donde herramientas especializadas actúan ante posibles amenazas. La integridad de nuestros datos y la estabilidad de nuestras operaciones están en juego, y nuestra tarea fundamental es preservar la confidencialidad y la integridad de la información que manejamos.

A lo largo de esta actividad nos sumergiremos en las motivaciones que nos llevan a adoptar soluciones de seguridad, explorando la evolución dinámica de las amenazas cibernéticas. La necesidad urgente de respuestas proactivas se hace evidente en un entorno donde anticipar y neutralizar posibles intrusiones son cruciales para evitar riesgos concretos.

Al adentrarnos en el mundo de la detección y prevención, descubriremos cómo estas tecnologías no solo bloquean accesos no autorizados, sino que también desempeñan un papel estratégico en la preservación de nuestra confianza digital y la sostenibilidad de nuestras operaciones cotidianas. En un entorno donde la seguridad es la clave del éxito digital, esta actividad nos provee con las herramientas y conocimientos necesarios para enfrentar los desafíos emergentes y asegurar un futuro cibernético resistente.

## Descripción

En el contexto presentado, se destaca la necesidad de implementar medidas de protección ante posibles ataques de explotación y acceso no autorizado a sistemas a través de la realización de auditorías en la red. La actividad propuesta implica la instalación y utilización de un software especializado para detectar y prevenir ataques de acceso al sistema y la red.

La importancia de la seguridad en este contexto radica en varios factores cruciales. En primer lugar, se busca prevenir los ataques de acceso, evitando que personas no autorizadas obtengan información confidencial o realicen acciones perjudiciales en los sistemas. Asimismo, la prevención de accesos no autorizados a las redes es esencial para garantizar la integridad y confidencialidad de los datos.

El monitoreo completo de la red también se destaca como un factor crítico. La capacidad de supervisar de manera exhaustiva la actividad en la red permite identificar posibles amenazas y responder de manera proactiva para mitigar riesgos antes de que se conviertan en problemas graves.

La actividad propuesta se alinea con la necesidad imperante de fortalecer la seguridad informática, abordando la prevención de ataques de acceso y la importancia del monitoreo constante para mantener la integridad y confidencialidad de los sistemas y la red. La implementación de herramientas tecnológicas especializadas juega un papel crucial en esta estrategia defensiva

## Justificación

La adopción de un software especializado para detectar y prevenir ataques de acceso en sistemas y redes se justifica por la creciente complejidad de las amenazas cibernéticas y la necesidad crítica de salvaguardar la integridad, confidencialidad y disponibilidad de la información. En el entorno actual, donde los ataques cibernéticos evolucionan constantemente, es esencial contar con herramientas avanzadas que puedan anticiparse a las tácticas de los actores malintencionados.

La implementación de esta solución ofrece una capa adicional de seguridad, permitiendo la identificación temprana de posibles vulnerabilidades y actividades sospechosas. La detección proactiva de amenazas minimiza el riesgo de intrusiones no autorizadas, protegiendo así los activos digitales y la privacidad de los usuarios.

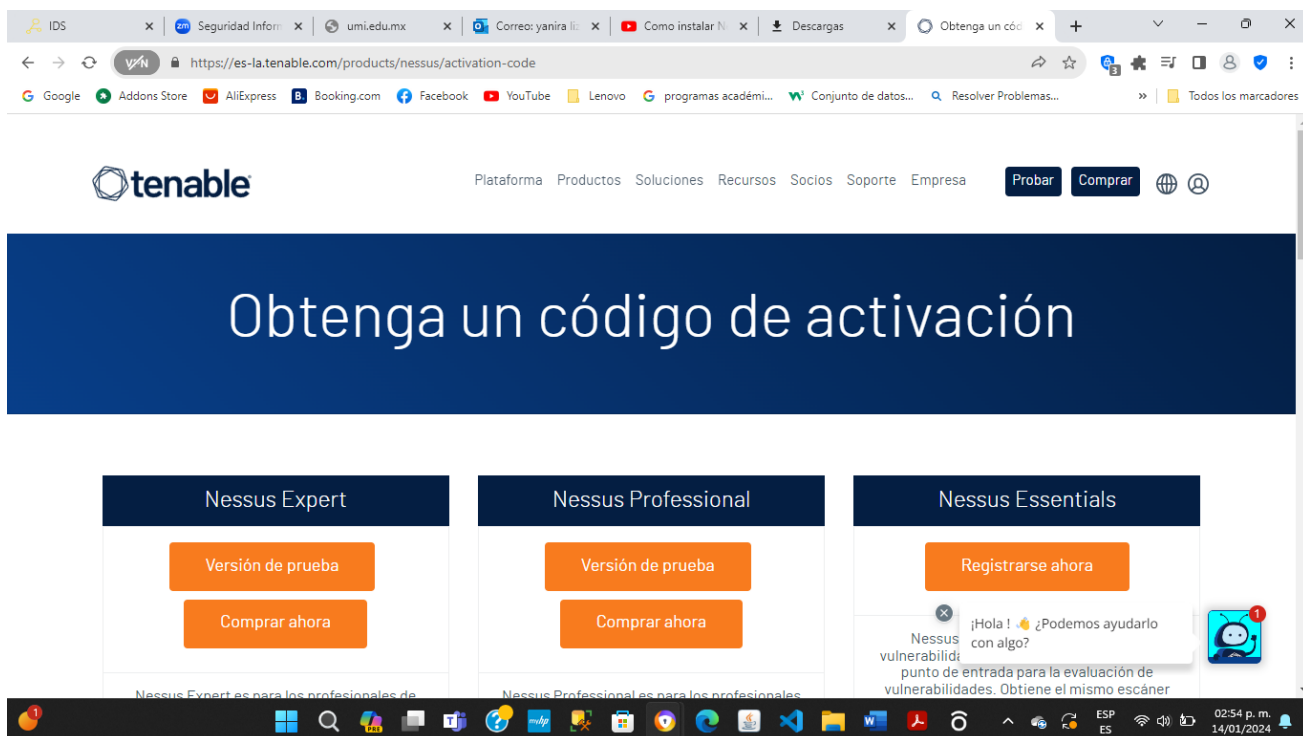
Además, en un mundo interconectado donde la infraestructura tecnológica juega un papel fundamental en las operaciones diarias de empresas y organizaciones, la prevención de accesos no autorizados a las redes se convierte en un componente esencial de la estrategia de seguridad. La inversión en este tipo de soluciones no solo fortalece la postura de seguridad, sino que también demuestra un compromiso serio con la protección de datos sensibles y la continuidad del negocio en el panorama digital actual. En definitiva, la adopción de esta solución es una medida proactiva y necesaria para garantizar la resiliencia de los sistemas ante las crecientes amenazas cibernéticas.

## Desarrollo:

En la siguiente imagen podemos observar cómo es que iniciamos con el proceso de registro y descarga de Nessus, la cual es una de las herramientas recomendadas para el desarrollo de la actividad.



A continuación, procedemos con obtención del código por lo cual debemos realizar para poder obtenerlo.



IDS x Seguridad Informa x umi.edu.mx x Como instalar N x Descargas x (1) Nuevos men x +

← → ↺ https://es-la.tenable.com/products/nessus/nessus-essentials

Google Addons Store AliExpress Booking.com Facebook YouTube Lenovo programas académi... Conjunto de datos... Resolver Problemas... >> Todos los marcadores

Plataforma Productos Soluciones Recursos Socio Soporte Empresa **Probar** **Comprar**

## Tenable Nessus® Essentials

Como parte de la familia Tenable Nessus, Tenable Nessus Essentials le permite escanear su entorno (hasta 16 direcciones IP por escáner) con la misma velocidad, evaluaciones exhaustivas y la misma comodidad de escaneo sin agentes que disfrutaron los suscriptores de Nessus.

Tenga en cuenta que Nessus Essentials no le permite realizar verificaciones de cumplimiento, auditorías de contenido, Live Results ni usar el dispositivo virtual de Nessus. Si necesita funcionalidades adicionales, puede comprar una suscripción a [Tenable Nessus Professional](#).

¿Utiliza Nessus Essentials para la educación? Regístrese en Nessus Essentials a través del programa [Tenable for Education](#) para comenzar.

¿Está interesado en saber cómo usar Nessus? Nuestro [curso bajo demanda](#) permite a los estudiantes, a través de una serie de videos específicos, desarrollar los bloques de construcción para el uso eficaz de la solución de evaluación de vulnerabilidades Nessus. Desde la detección de activos hasta la evaluación de vulnerabilidades y el cumplimiento, los participantes aprenderán a usar eficazmente Nessus en diversos casos de uso de negocios. [Más información](#).

Nessus es **ESTÁNDAR DE ORO** para evaluación de vulnerabilidades  
**PRUEBE NISSUS GRATIS POR 7 DÍAS**

[PRUEBA AHORA](#)

Regístrese para obtener un código de activación

Nombre  Apellido

Correo electrónico laboral

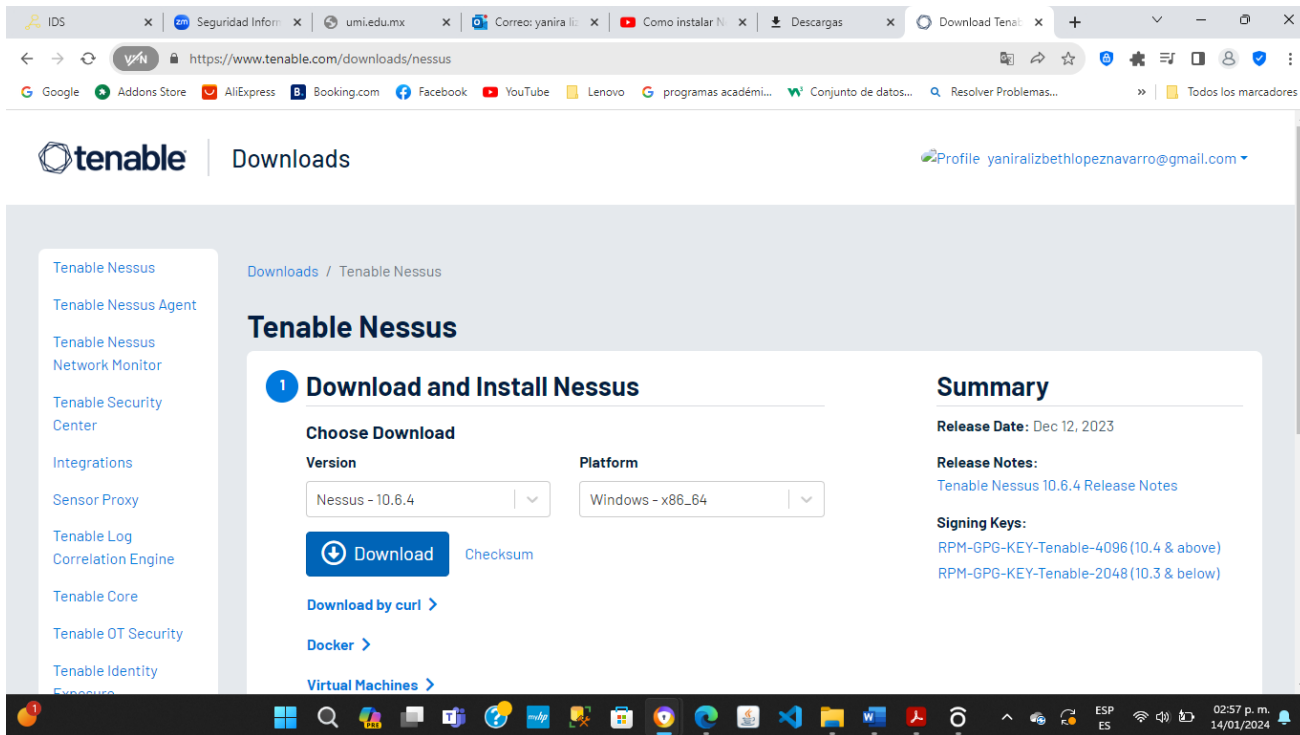
☐ Marque para recibir actualizaciones de Tenable

Tenable solo procesará sus datos personales como se describe en su Política de privacidad.

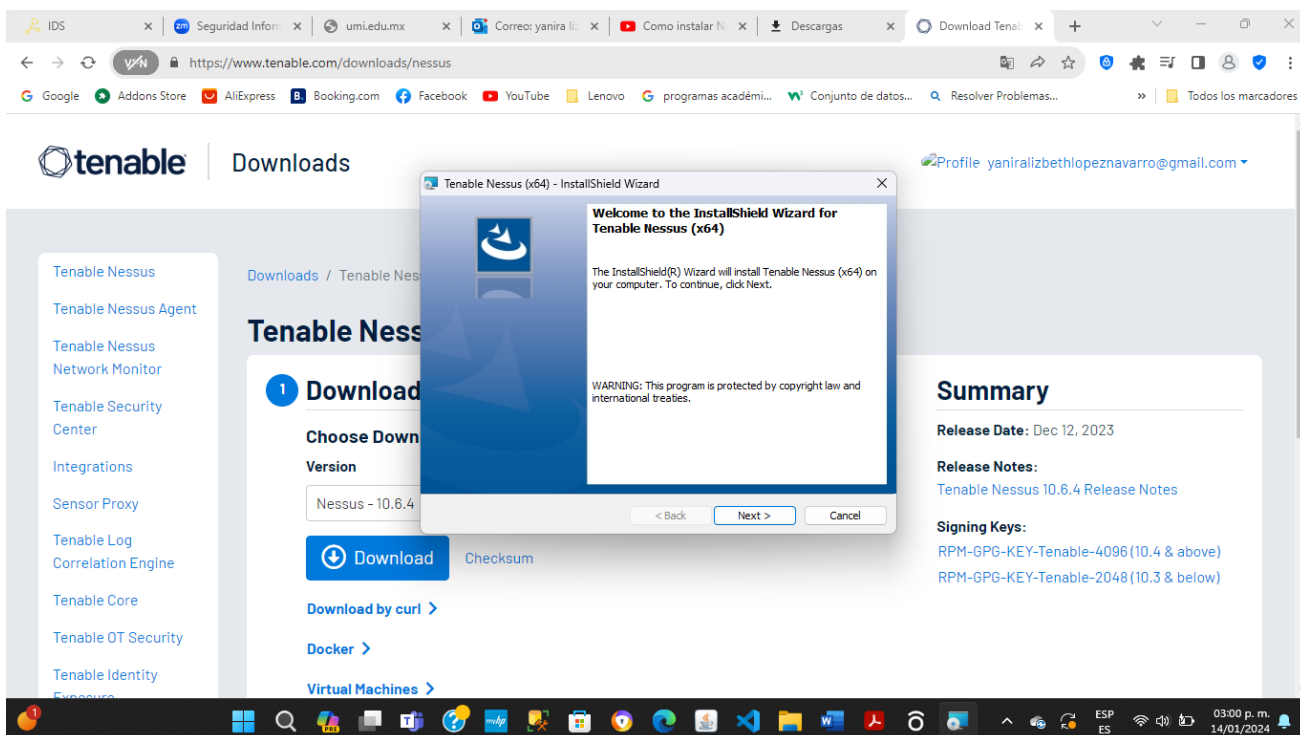
¡Hola! ¿Podemos ayudarlo con algo?

02:56 p. m. 14/01/2024

Una vez que ya contamos con el registro nos muestra la siguiente pantalla la cual nos permite continuar con la descarga de Nessus.

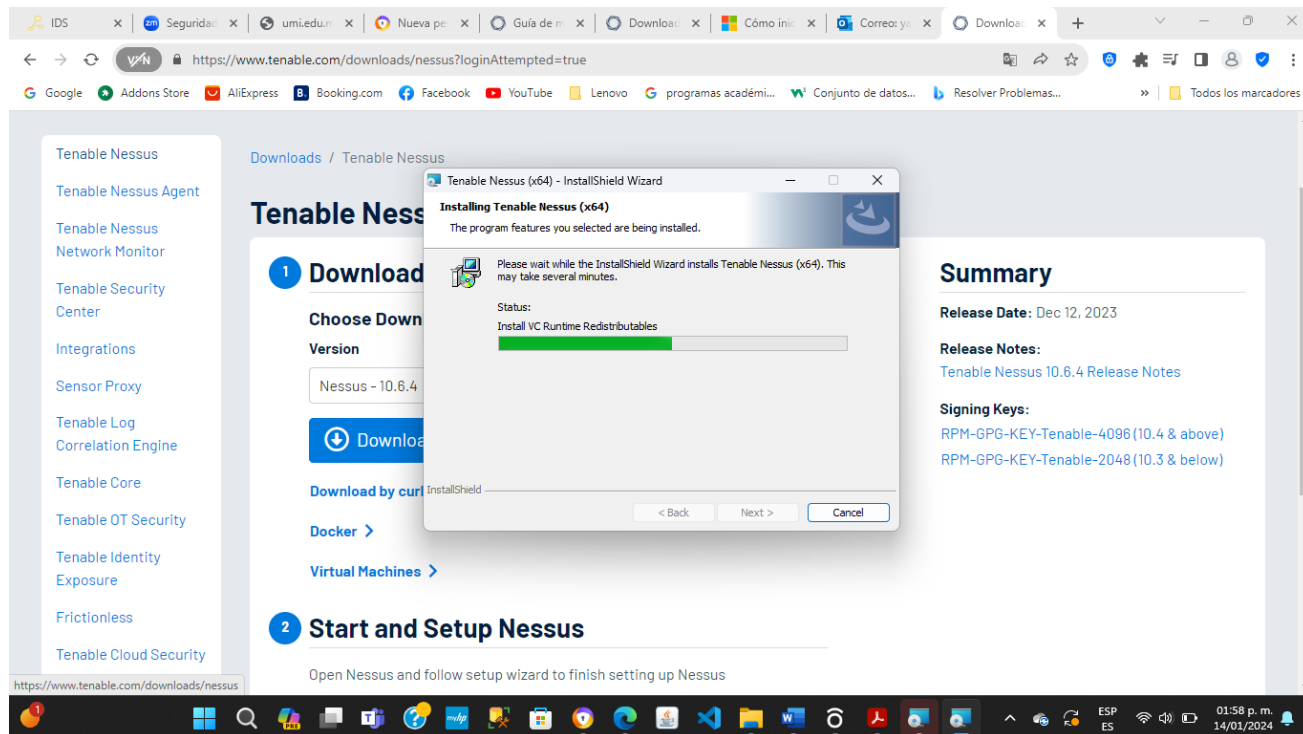


Una vez que ya se descargó el archivo de Nessus continuamos con la instalación, como nos lo muestra la pantalla siguiente.

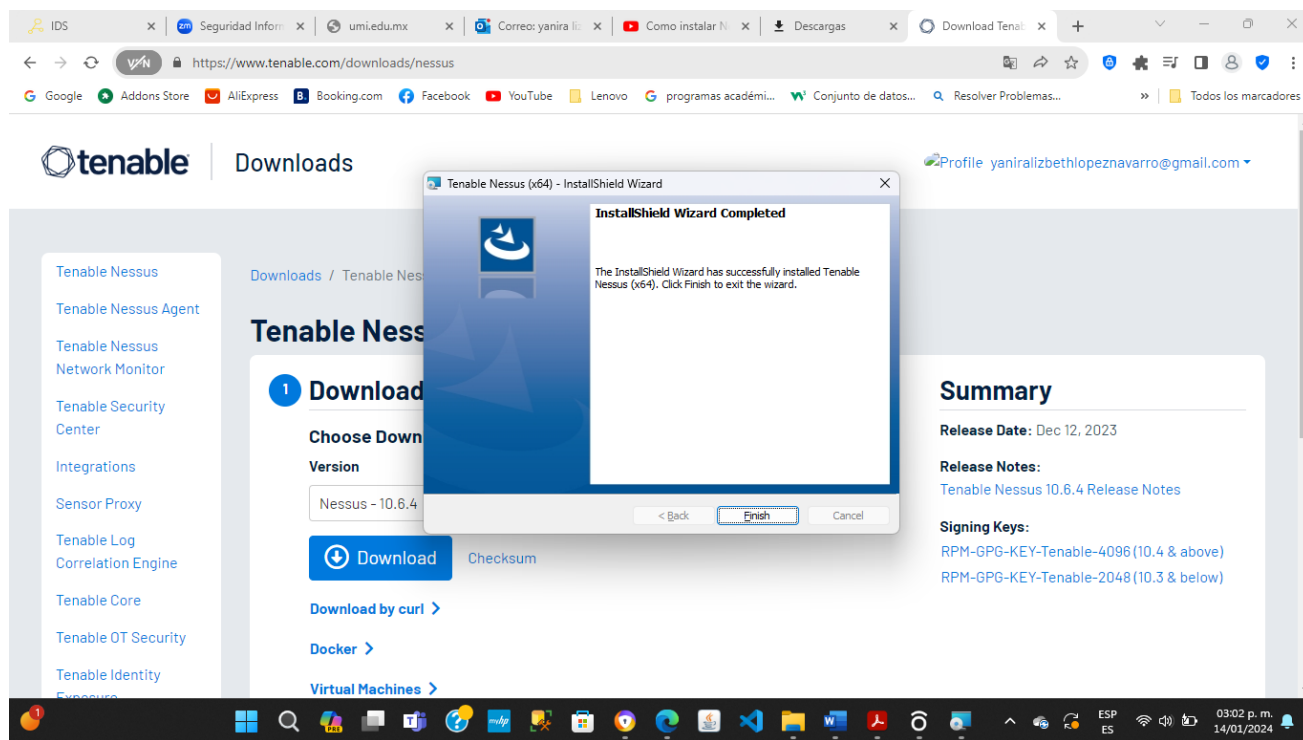




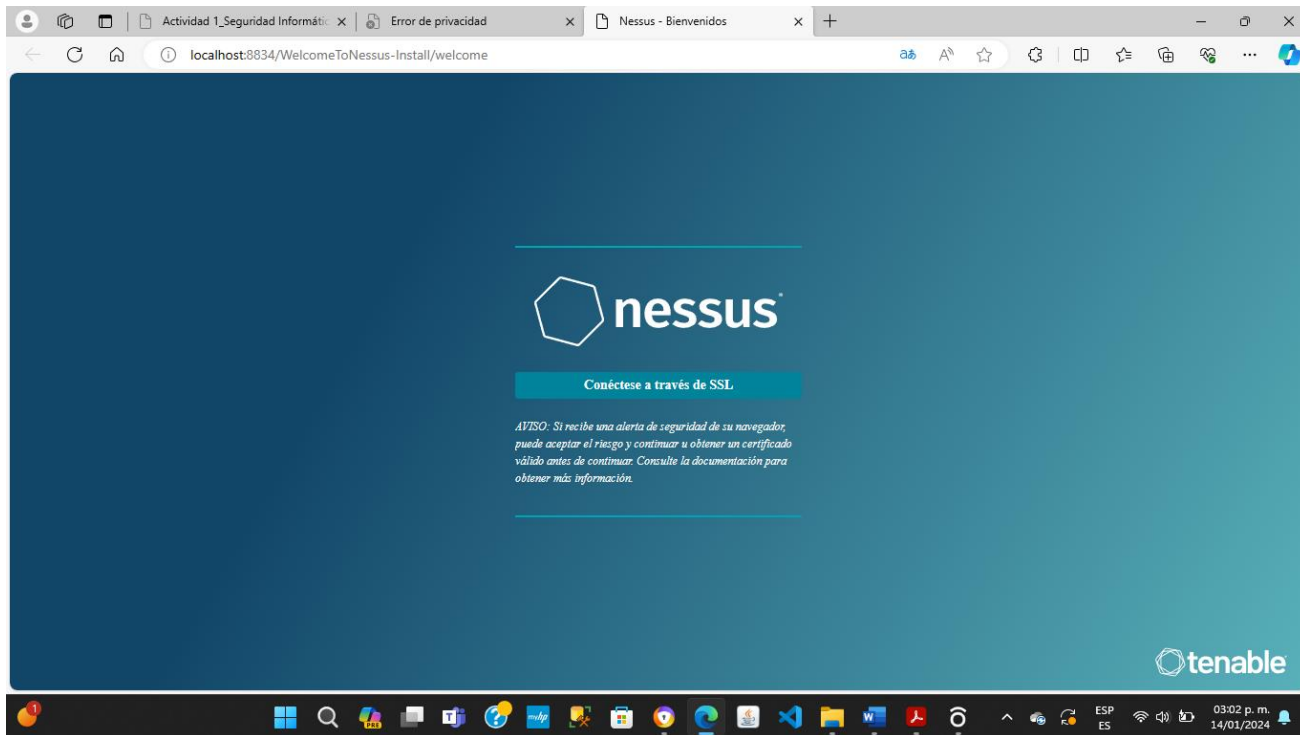
A continuación, podemos observar el avance de la instalación del programa Nessus.



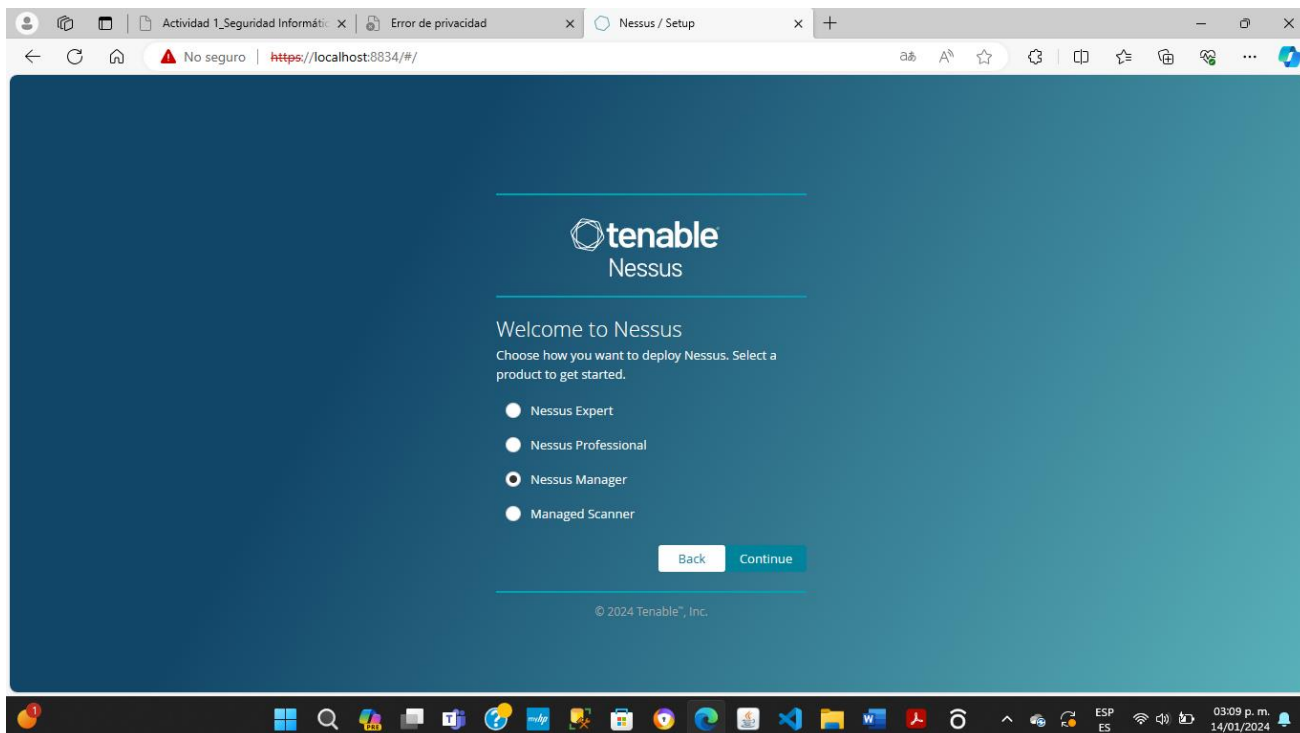
En seguida nos muestra la siguiente pantalla la cual da por concluida la instalación y procedemos a finalizar.



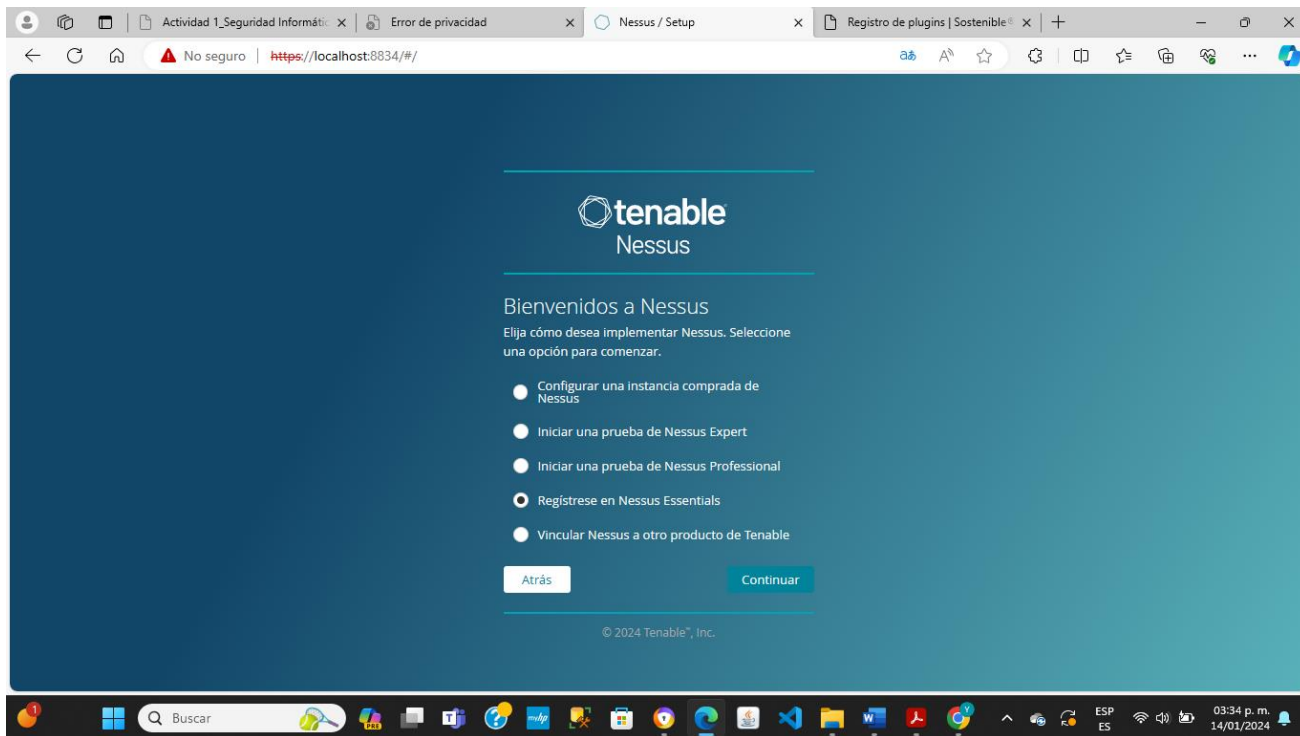
Una vez que finalizamos la instalación nos arroja la siguiente pantalla en la cual debemos seleccionar conectarse a través de SSL.



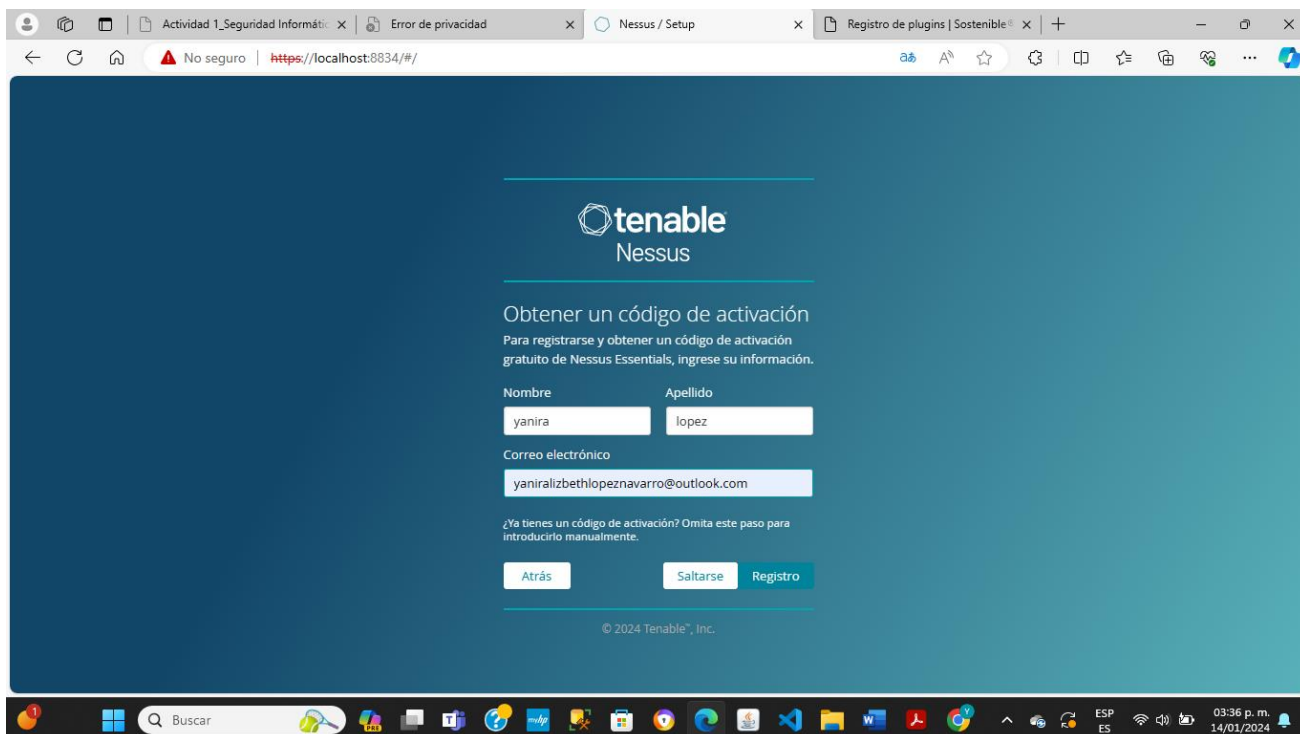
A continuación, nos arroja el mensaje de bienvenida a Nessus.



En seguida nos muestra una serie de opciones, de las cuales debemos seleccionar, Registrarse en Nessus Essentials y continuar.

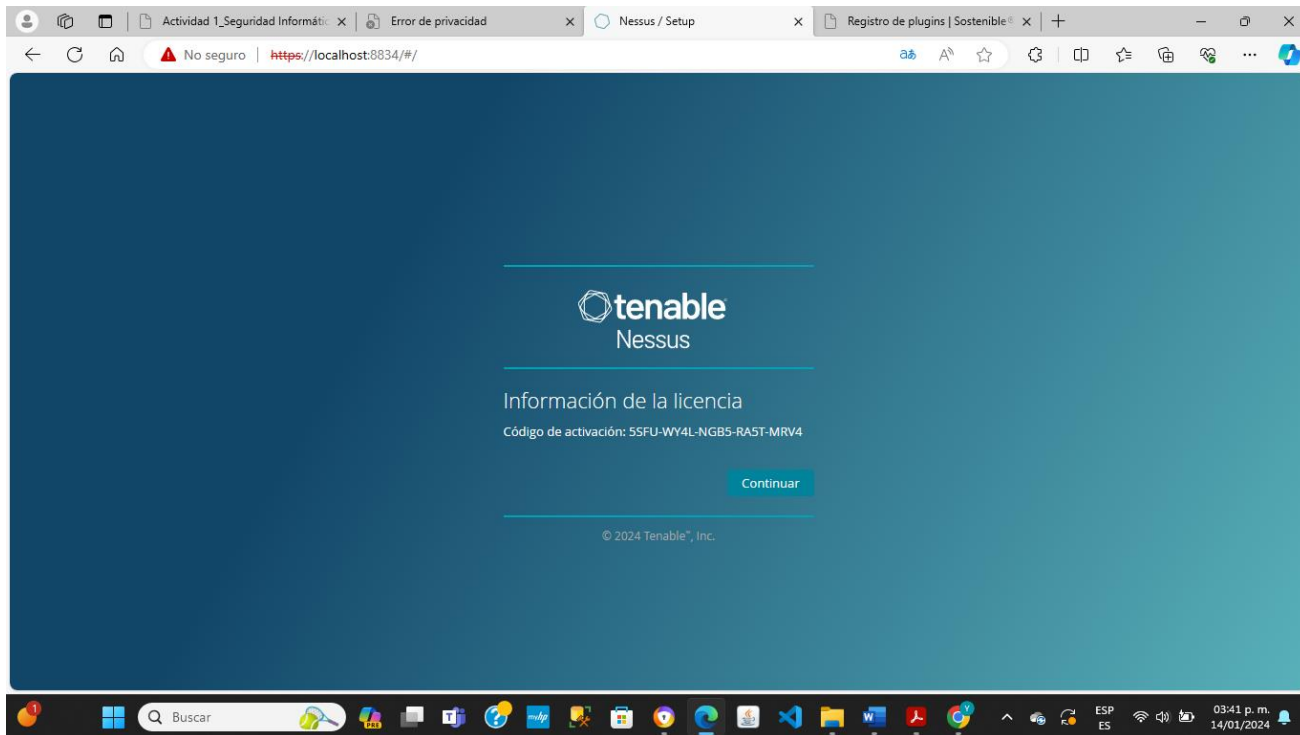


En la siguiente imagen procedemos con el registro e introducimos la información solicitada, lo cual nos permitirá obtener un código de activación.

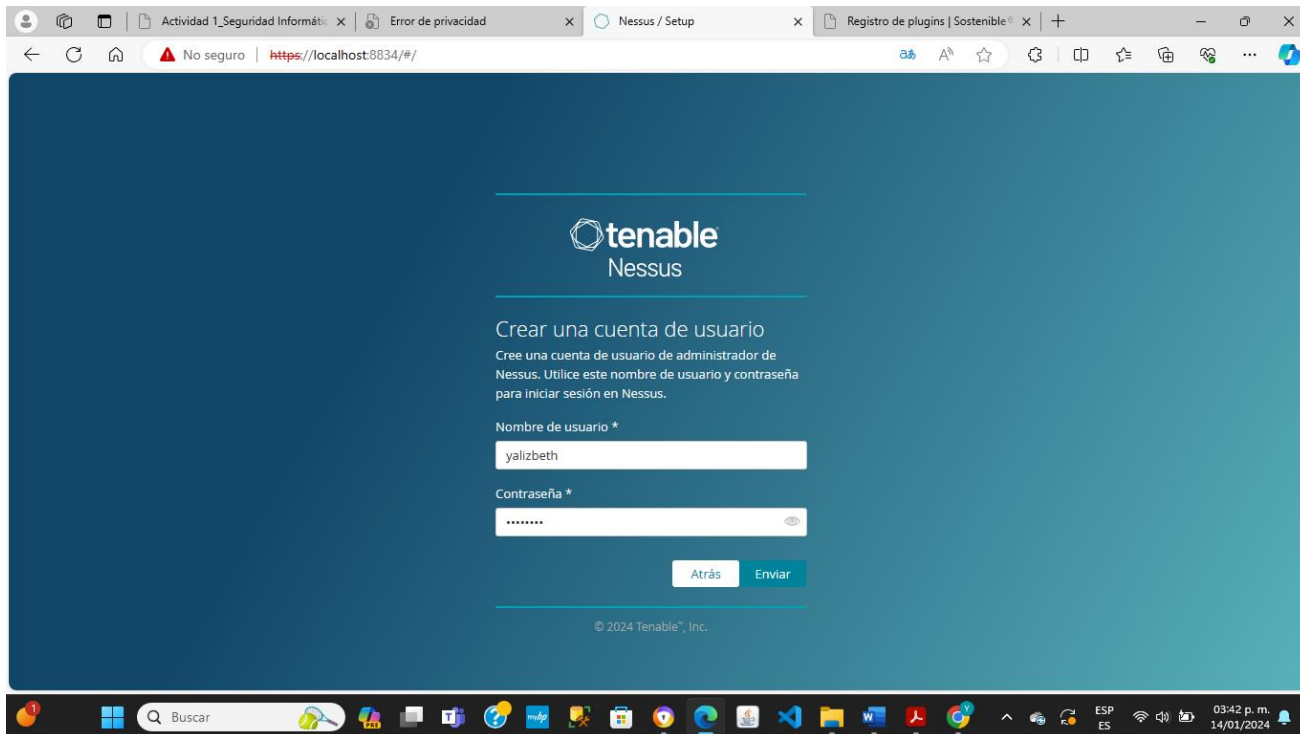


En seguida nos muestra el código de activación.

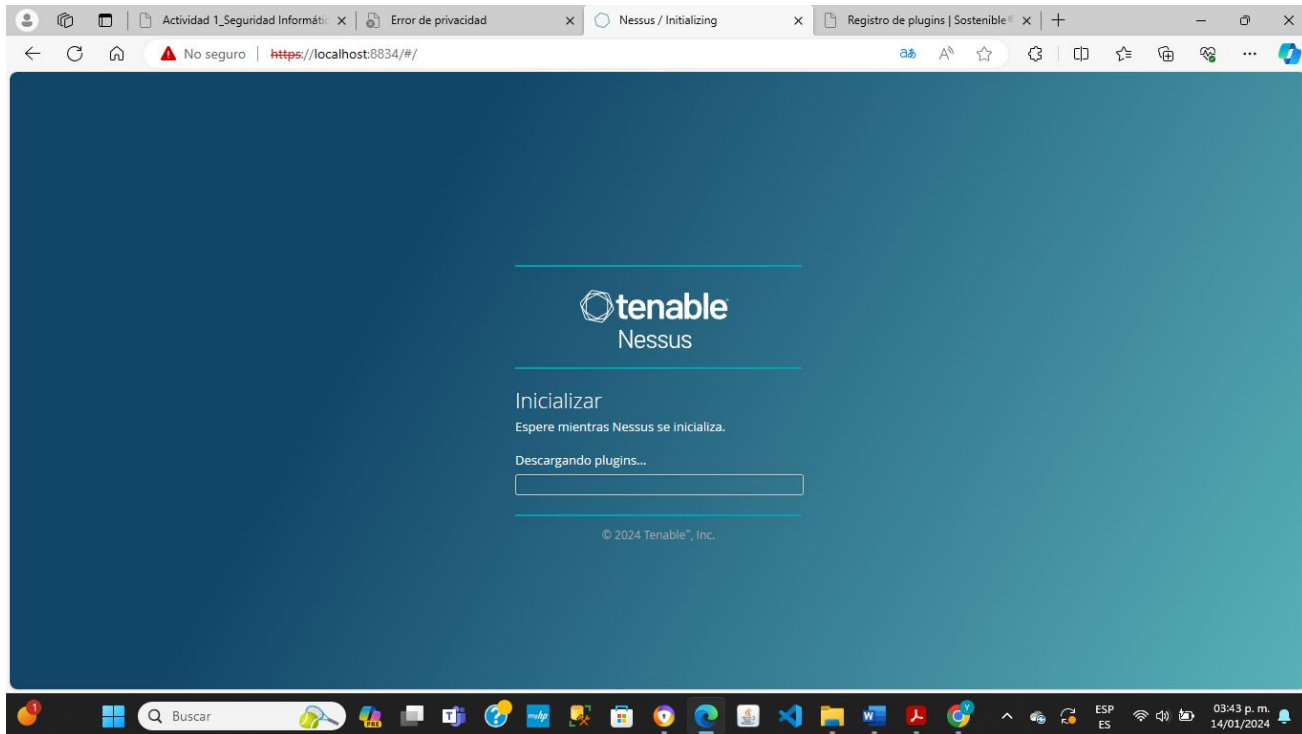
5SFU-WY4L-NGB5-RA5T-MRV4



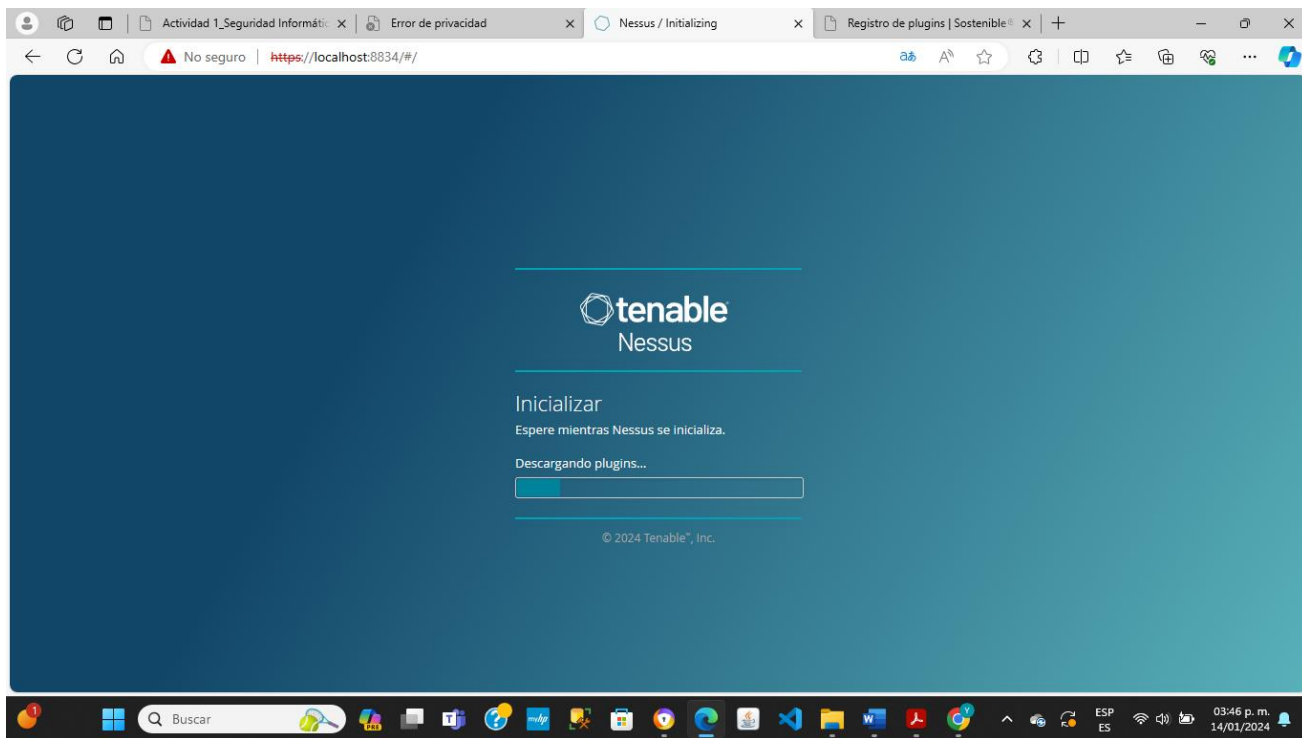
Una vez que ya contamos con nuestro código de activación introducimos un usuario y contraseña.



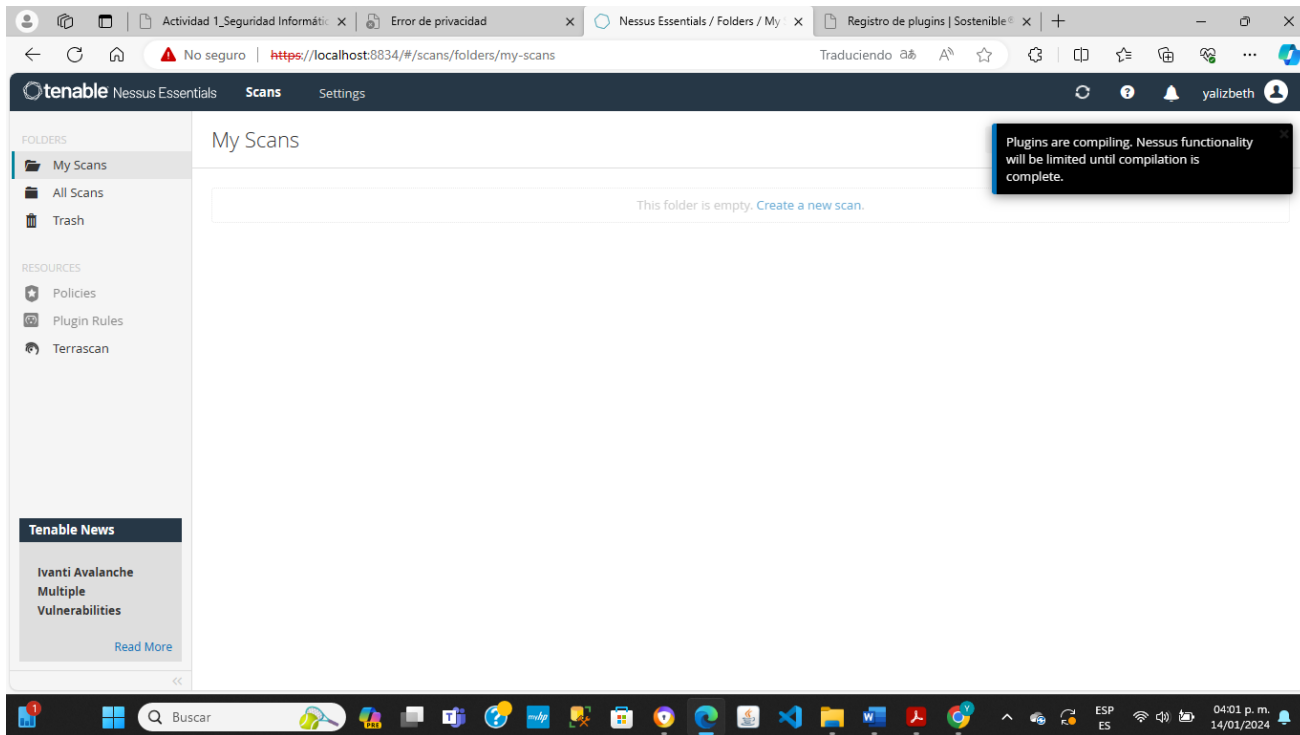
En seguida nos muestra el inicio de la descarga.



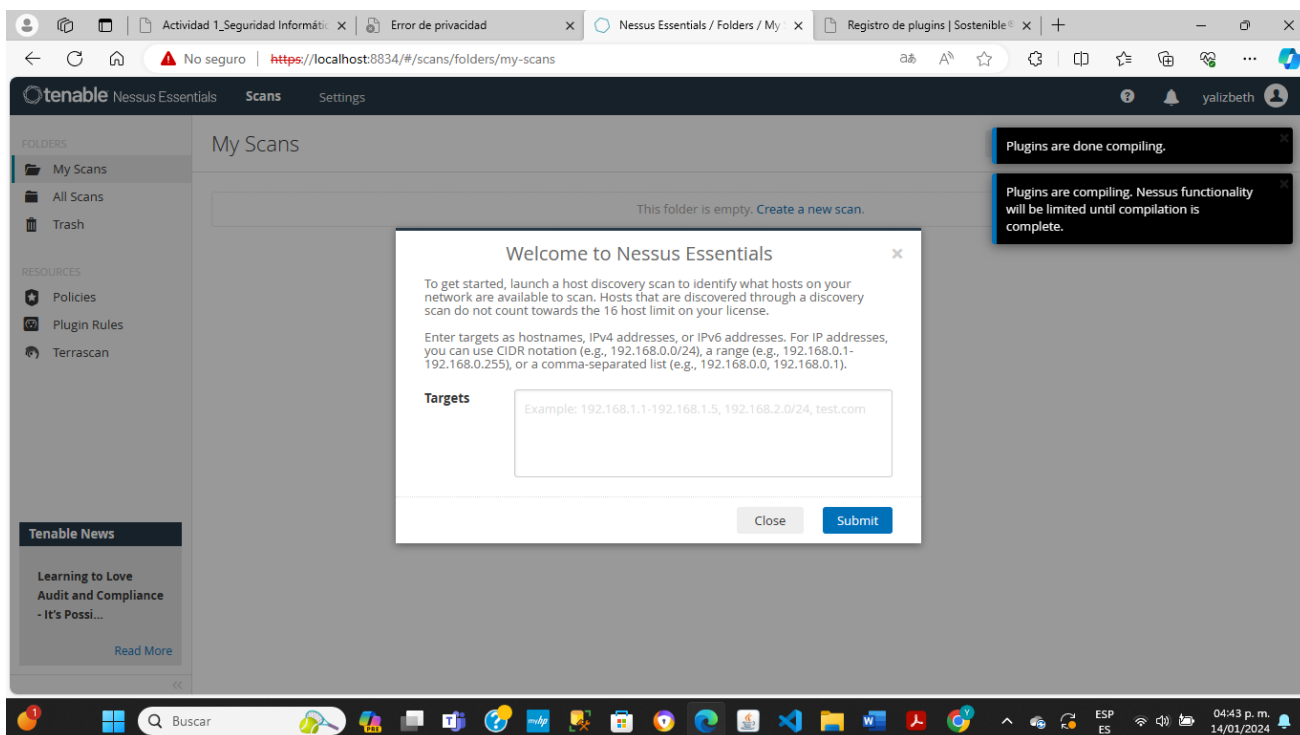
A continuación, podemos observar el avance de la instalación de Nessus.



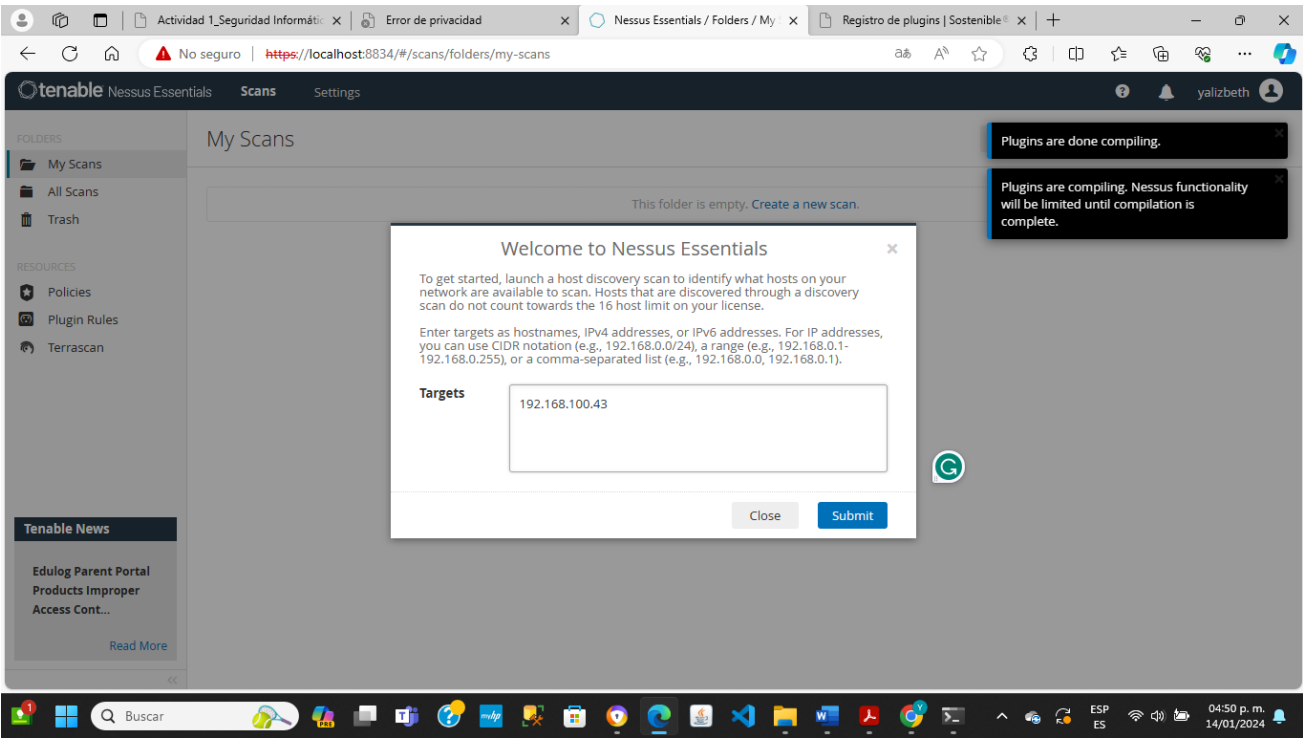
Una vez concluida la instalación nos muestra la siguiente pantalla en la cual podemos observar que se está compilando.



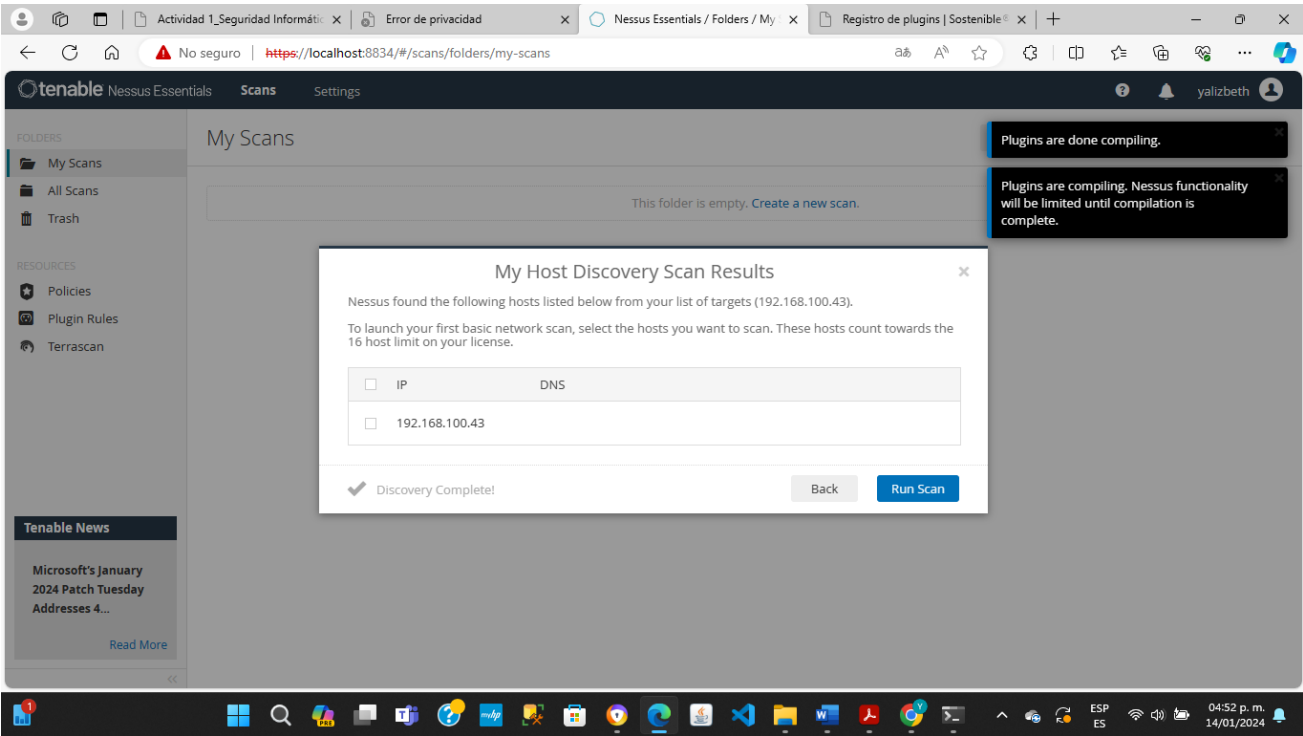
En la siguiente imagen podemos observar que se ha terminado el proceso de compilación y nos arroja un recuadro en el cual nos solicita la IP del equipo que vamos a analizar.



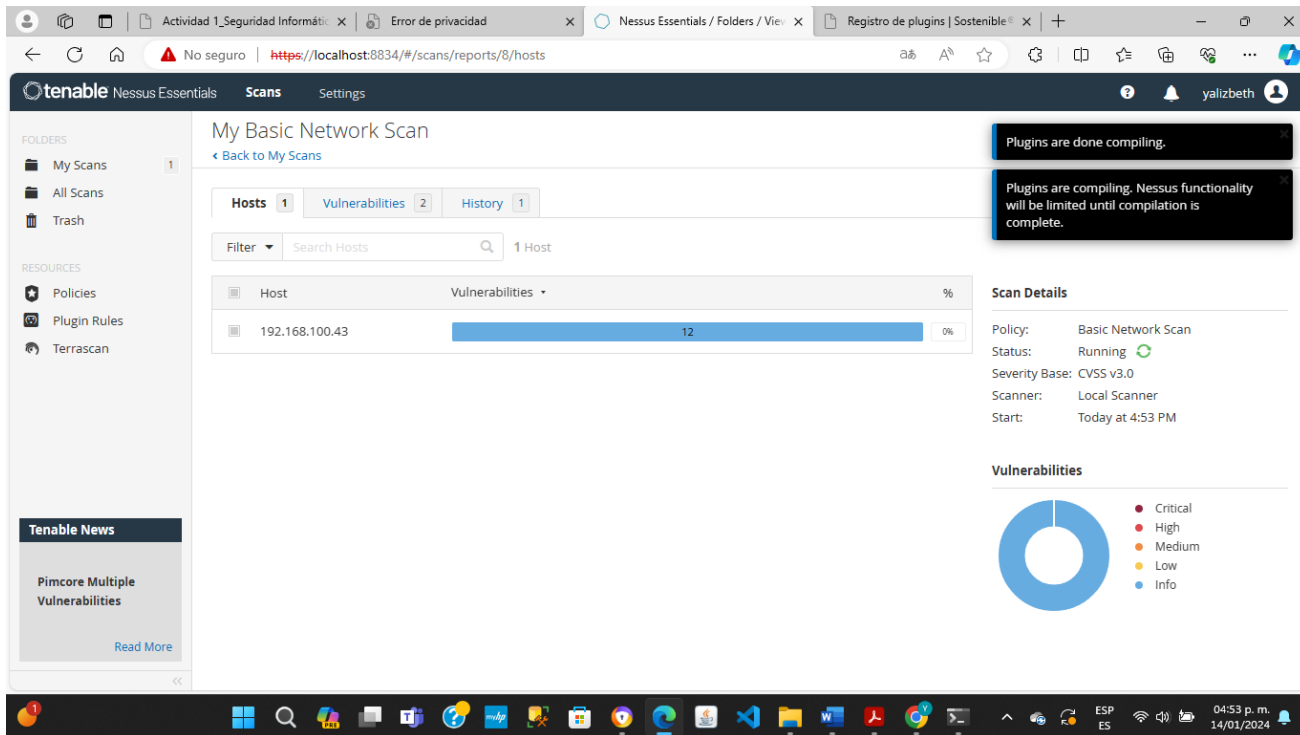
En seguida ingreso la IP de mi equipo.



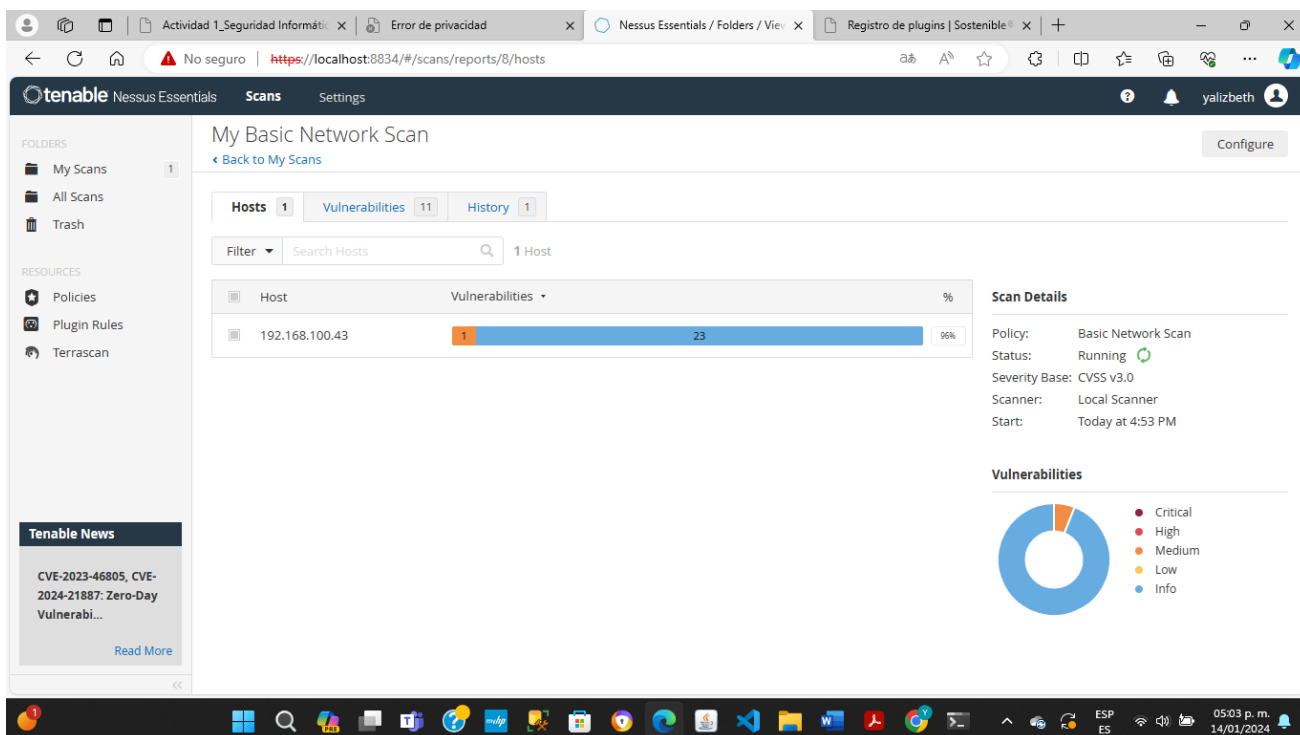
En seguida confirmamos el inicio de mi analizar.



En a la siguiente imagen nos muestra el inicio del análisis de mi equipo, el cual apenas va dar inicio al informe, es por ello que solo podemos observar en el circulo el color azul.

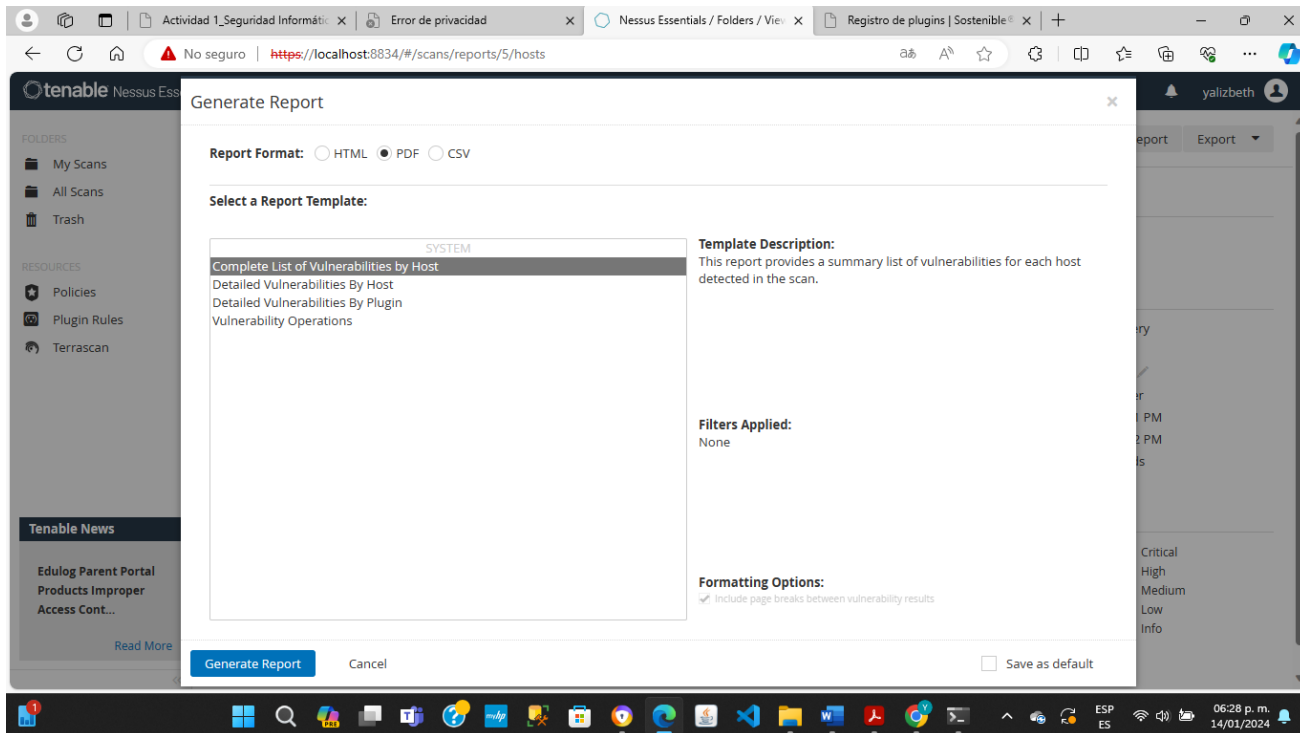


A continuación, la siguiente imagen nos muestra el avance de nuestro análisis, el cual aún que aún no esté concluido nos refleja 11 vulnerabilidades.

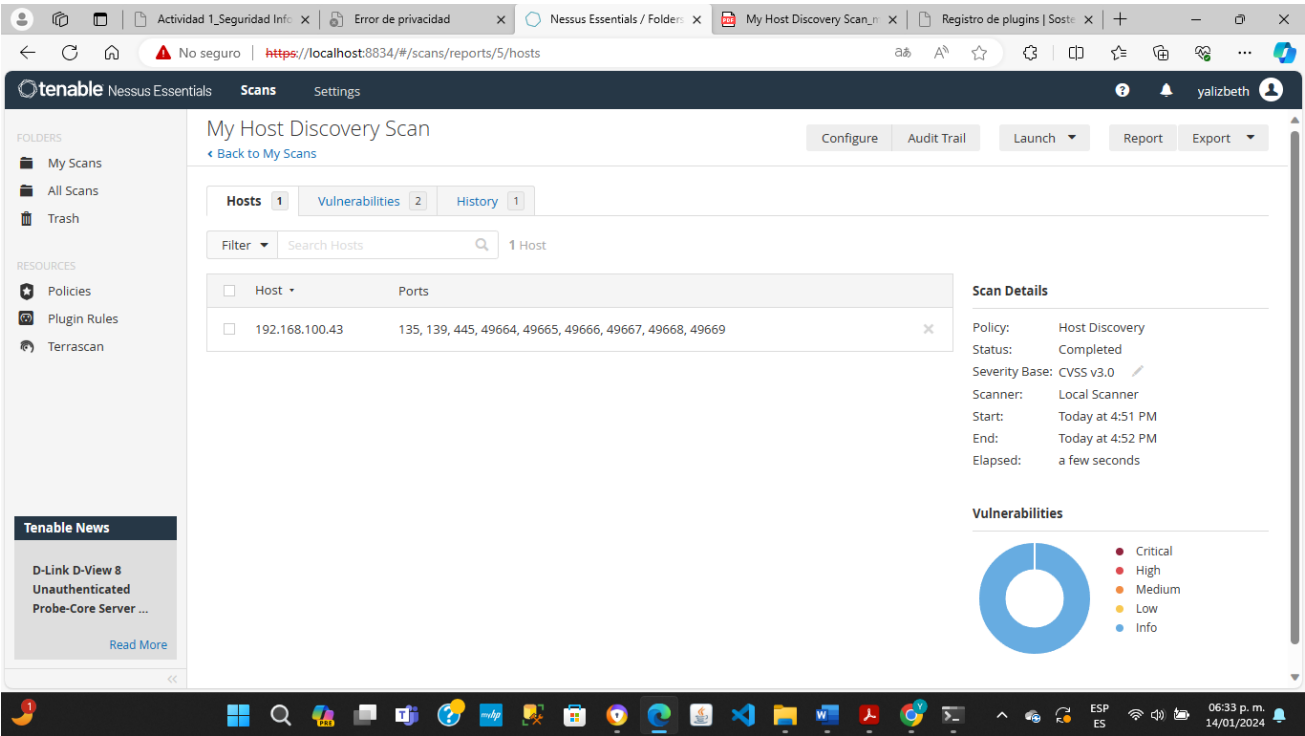




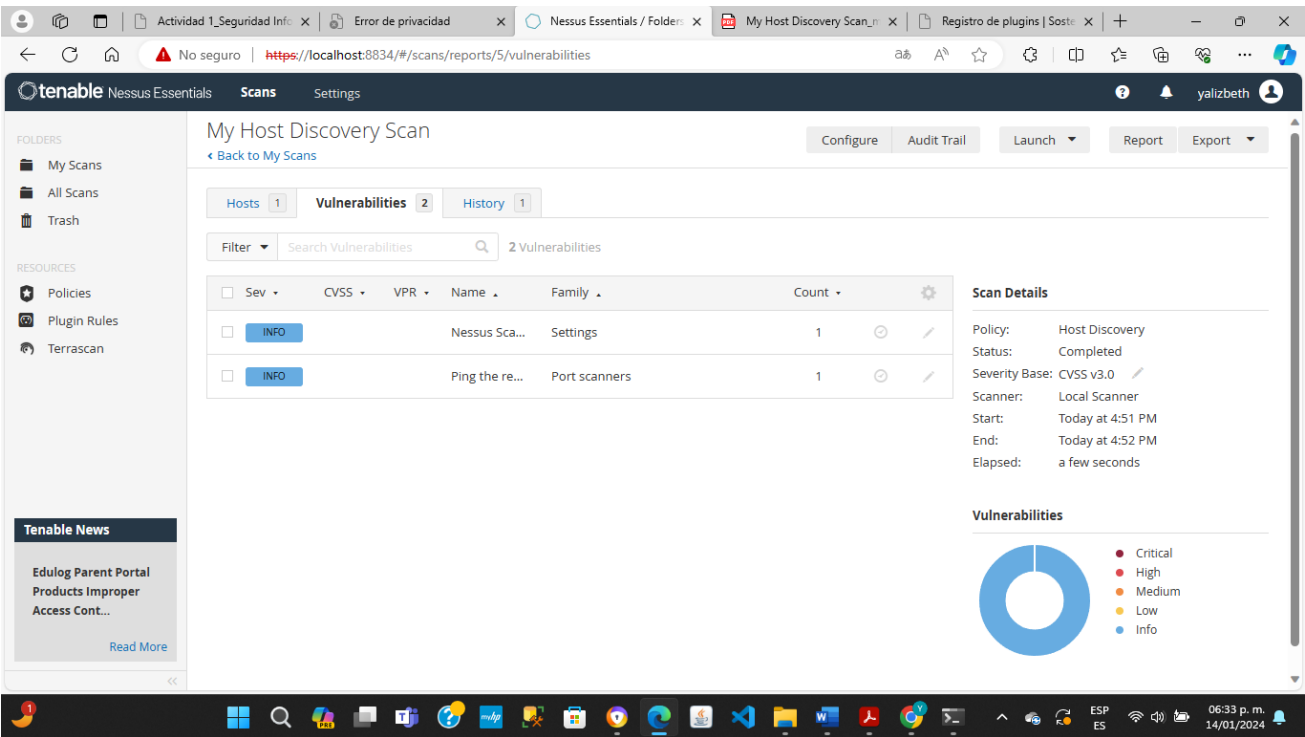
Una vez concluido el análisis nos arroja la siguiente pantalla la cual nos permite generar el reporte y expórtalo PDF.



# Incidencias encontradas



En la siguiente imagen se muestra las vulnerabilidades encontradas.



En seguida podemos observar el detalle de la hora en que inicio y concluyo en proceso de análisis.

tenable Nessus Essentials Scans Settings yalizbeth

My Host Discovery Scan

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 2 History 1

Search History 1 History

<input type="checkbox"/>	Start Time	Last Scanned	Status
<input type="checkbox"/>	Current Today at 4:51 PM	Today at 4:52 PM	✓ Completed

**Scan Details**

Policy: Host Discovery  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 4:51 PM  
End: Today at 4:52 PM  
Elapsed: a few seconds

**Vulnerabilities**

1 Critical  
1 High  
1 Medium  
1 Low  
1 Info

Tenable News

SQL Injection in My Calendar WordPress Plugin

Read More

06:34 p.m. 14/01/2024

## Reporte

Enseguida se muestra el reporte obtenido durante el análisis el cual fue exportado desde Nessus.



# My Host Discovery Scan

Report generated by Nessus™

Sun, 14 Jan 2024 16:52:11 Mountain Standard Time (Mexico)

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.100.43 .....	4
------------------------	---

*Nessus Essentials*

---

## **Vulnerabilities by Host**

---



Vulnerabilities

T

otal: 2

SEVERIT	CVSS V3.0	VPR SCORE	PLUGIN NAME
INFO	N/A -	19506	Nessus Scan Information
INFO	N/A -	10180	Ping the remote host

\* Indicates the v3.0 score was not available; the v2.0 score is shown

---

192.168.100.43



## Análisis e Identificación de mejoras.

-Es crucial establecer un proceso regular de revisión y mitigación basado en los resultados de escaneos, priorizando aquellas áreas que puedan representar posibles riesgos futuros. La mejora continua en este aspecto fortalecerá la resistencia del sistema frente a amenazas potenciales.

-Es recomendable implementar medidas de seguridad que limiten la visibilidad externa, incluso para información de bajo riesgo como los pings. Esto contribuirá a un perfil de seguridad más robusto y a la reducción de la exposición a posibles ataques.

-Aunque la información recopilada, incluso si es informativa, requiere una auditoría más refinada. Es esencial garantizar que los datos recopilados sean pertinentes y no revelen información sensible innecesaria. Este refinamiento contribuirá a mantener la privacidad y a reducir la superficie de ataque del sistema.

-Mantener registros actualizados facilita la identificación y corrección eficiente de posibles riesgos, promoviendo así una seguridad más sólida.

## Conclusión

El participar en la actividad centrada en detectar y prevenir ataques de acceso no solo se presenta como algo clave en el ámbito laboral, sino también como una herramienta indispensable para el día a día. En el trabajo, implementar medidas proactivas de seguridad no es solo un escudo para nuestros sistemas, sino una forma de garantizar la integridad de información vital y asegurar que todo siga funcionando sin contratiempos. Esta práctica no es solo una reacción a las amenazas que enfrentamos hoy, sino una inversión para mantener la solidez y el éxito a largo plazo de la empresa u organización.

En nuestra vida cotidiana, la seguridad digital se convierte en algo crucial. Entender las posibles amenazas y adoptar prácticas seguras no solo protege nuestra privacidad personal, sino que también aporta a la seguridad general en el vasto paisaje digital compartido por la sociedad, la actividad que llevamos a cabo no solo responde a peligros inmediatos, sino que es una contribución esencial para construir un entorno digital más seguro y resistente, tanto en el trabajo como en nuestra vida diaria. Este compromiso nos empodera, no solo como profesionales, sino como individuos navegando en un mundo digital en constante evolución.

## Referencias

Ingeniería en desarrollo de software. Universidad México Internacional. Recuperado el día 08 de enero de 2024, <https://umi.edu.mx/coppel/IDS/mod/scorm/player.php>

Global, A. (2024, 9 enero). *Video 1 DynaTrace Synthetic Monitoring Monitorización de disponibilidad y rendimiento de las aplicaciones web..mp4* [Vídeo]. Vimeo.

<https://vimeo.com/660530504/e6e2591340>

Global, A. (2024b, enero 14). *Video 2 Auditoría de vulnerabilidades en la red con Nessus* [Vídeo].

Vimeo. <https://vimeo.com/660530360/ad1982a98c>