

# **Actividad 1 - Detección y prevención de ataques de acceso**

## **Seguridad Informática 2**

### **Ingeniería en Desarrollo de Software**

**Tutor: Jessica Hernández Romero**

**Alumno: Fernando Pedraza Garate**

**Fecha: 19 de mayo 2024**

# Índice

---

## Etapa 1 – Detección y prevención de ataques de acceso

○ Introducción.	Pág. 3
○ Descripción	Pág. 4
○ Justificación	Pág. 5
○ Desarrollo	Pág. 6 - 17
• Incidencias encontradas	
• Reporte	
• Análisis de identificación de mejoras	
○ Conclusión	Pág. 18
○ Referencias	Pág. 19

# 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. (*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 el accesos a las redes, instalando y utilizando un software que permita detectar y prevenir ataques de acceso al sistema y a la red, auditando sus vulnerabilidades ante un posible ataque de virus, a accesos no permitidos o percances en la red, y así poder generar un reporte desde la herramienta a utilizar que demuestre el resultado detallado del análisis generado.

# 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.

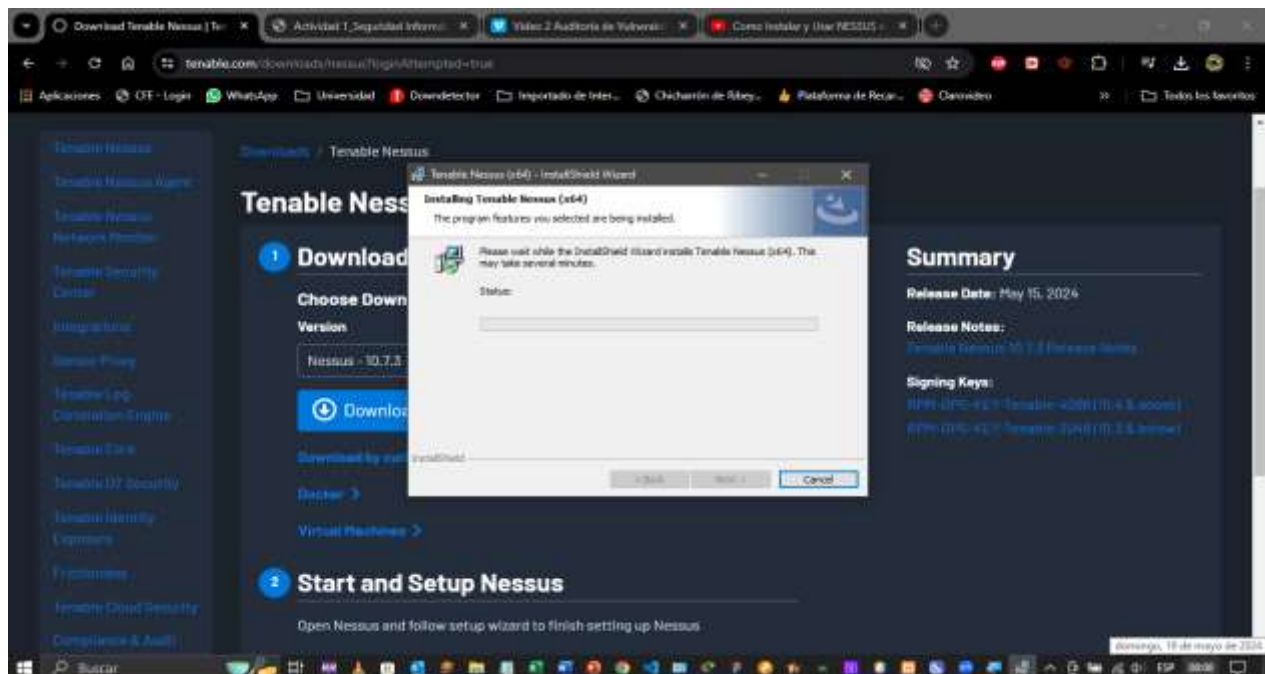
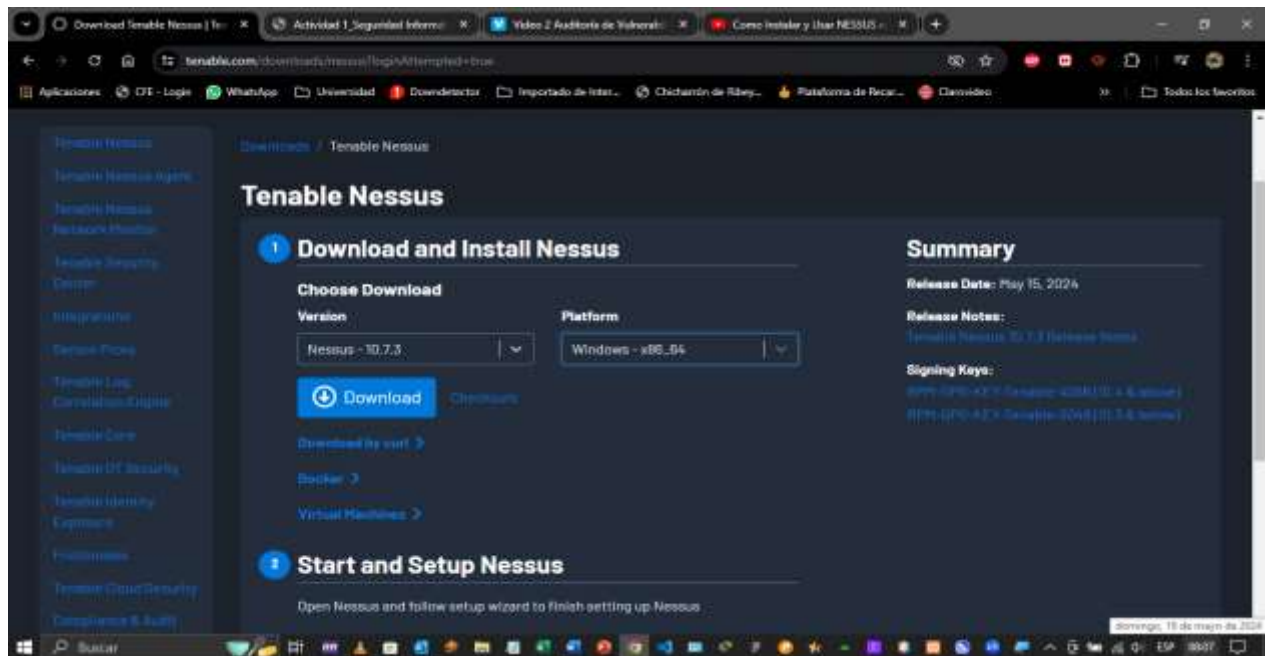
Las herramientas y técnicas que pueden ayudar a cumplir con esta ardua labor son los Sistemas de Detección de Intrusos (IDS) que ayudan a monitorear y analizar el tráfico de red identificando actividades sospechosas, los Sistemas de Prevención de Intrusos (IPS) además de detectar ayudan a prevenir ataques 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.

(ChatGPT, n.d.)

# Desarrollo.

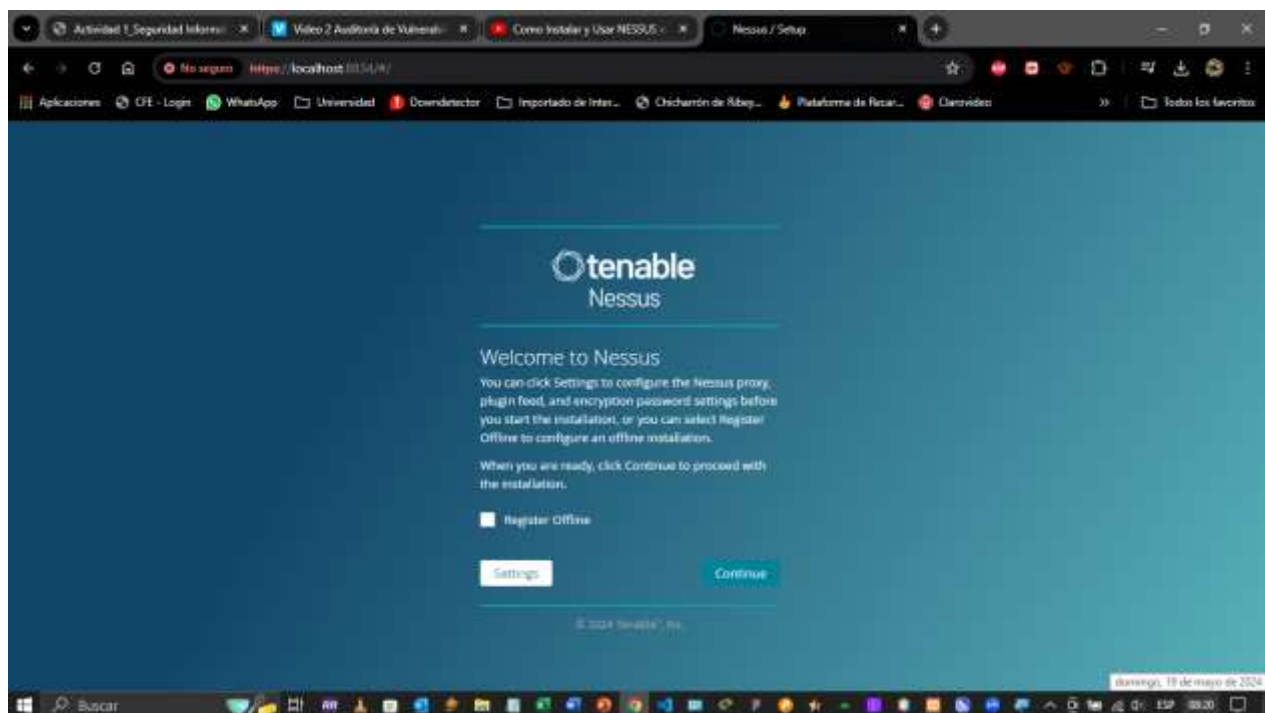
Se descarga e instala el programa a utilizar desde el siguiente enlace:

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

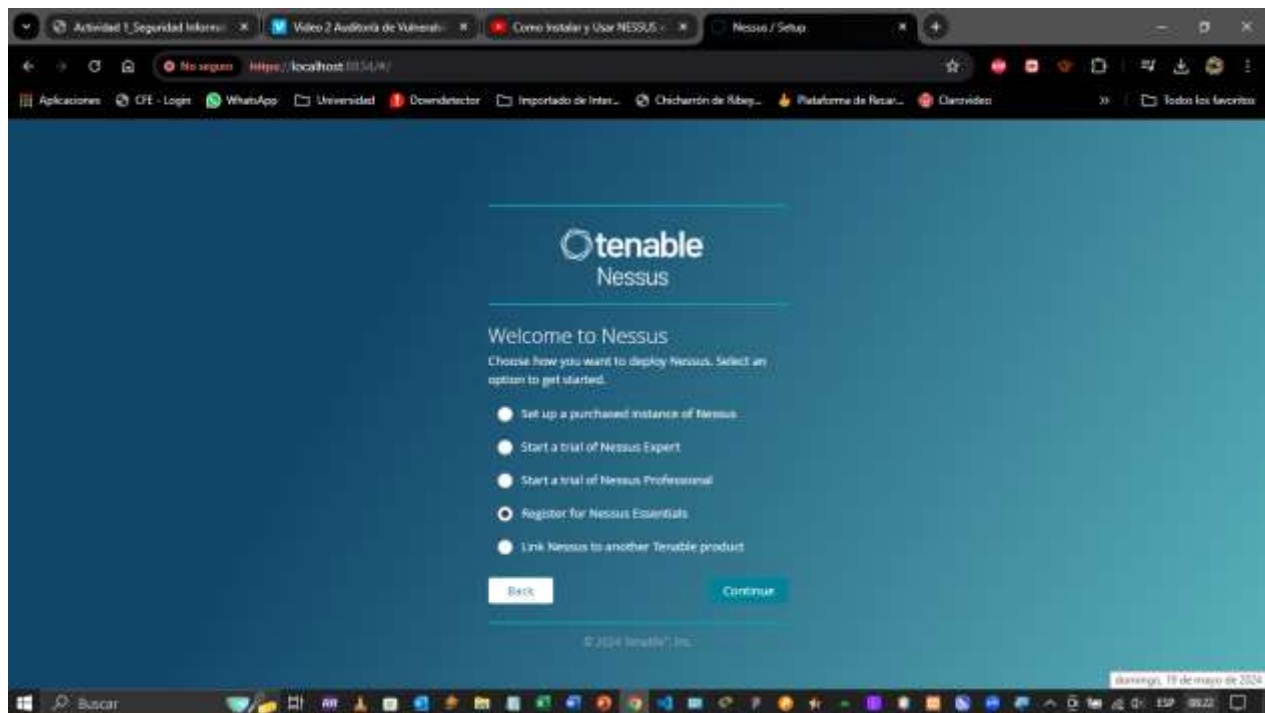




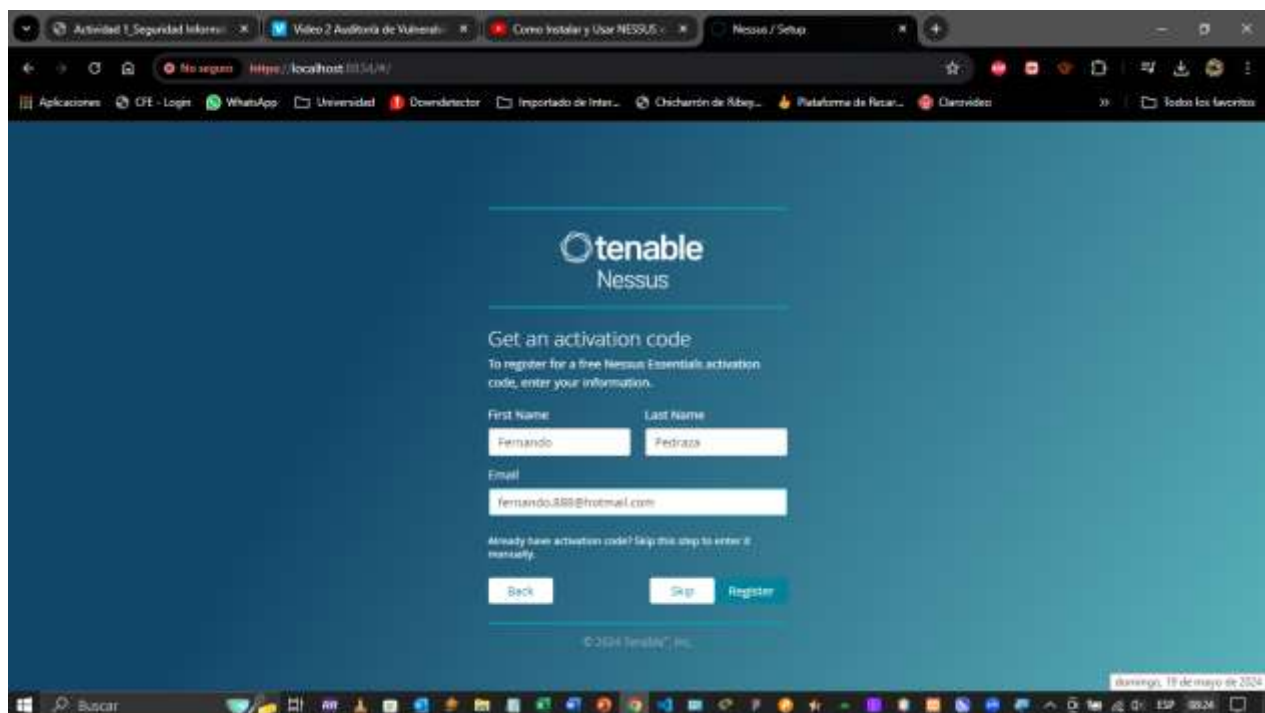
Al concluir se hace la conexión vía SSL con nessus



Se continua con el registro en línea

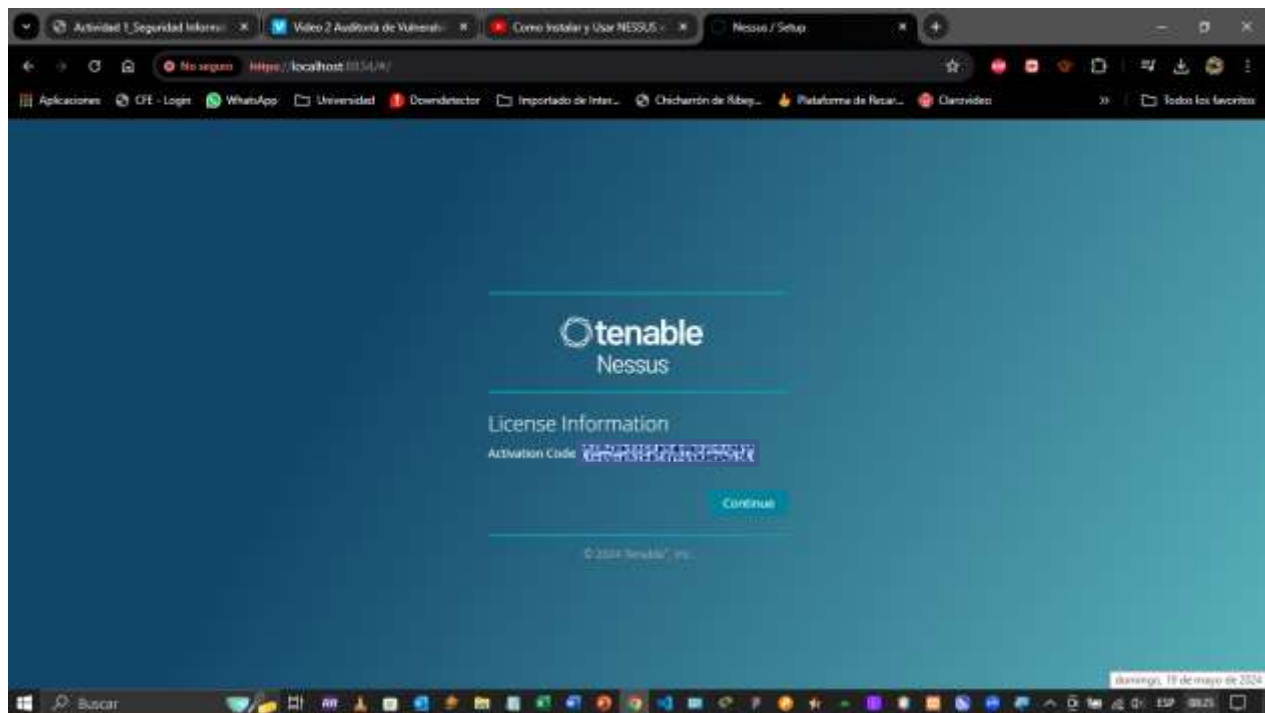


Se selecciona el registro para Nessus Essentials

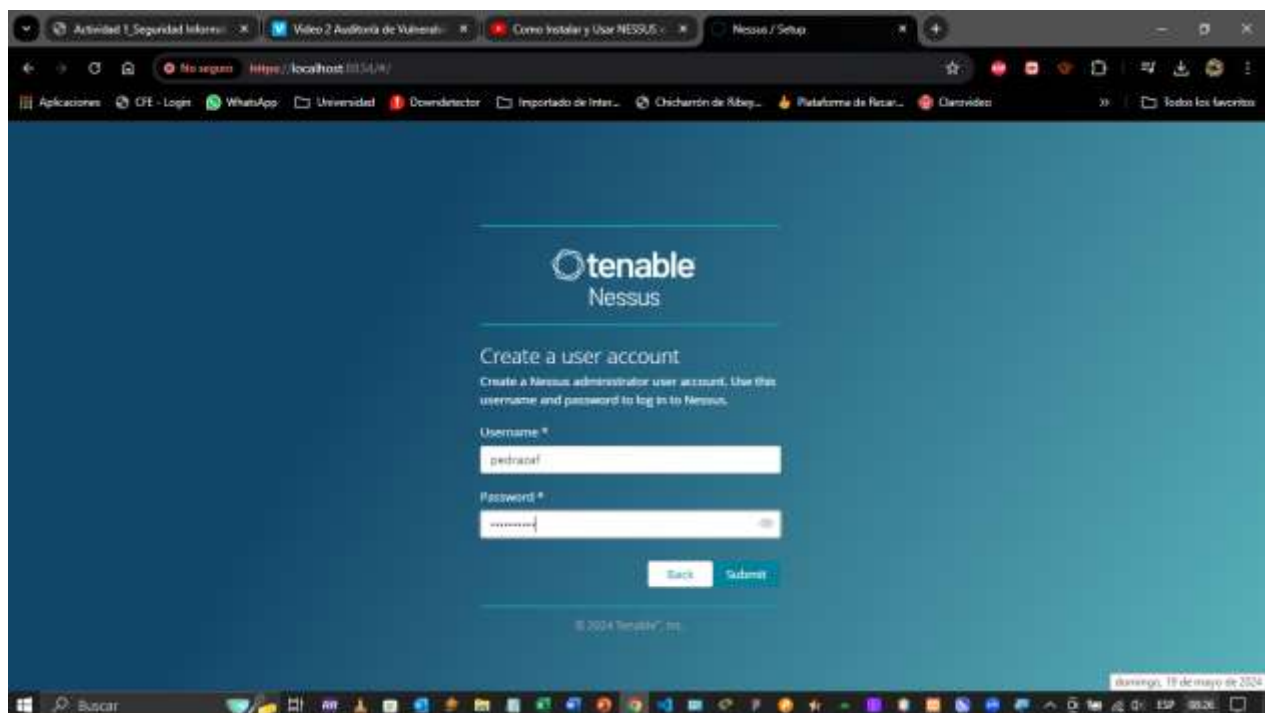


Se registran los datos solicitados

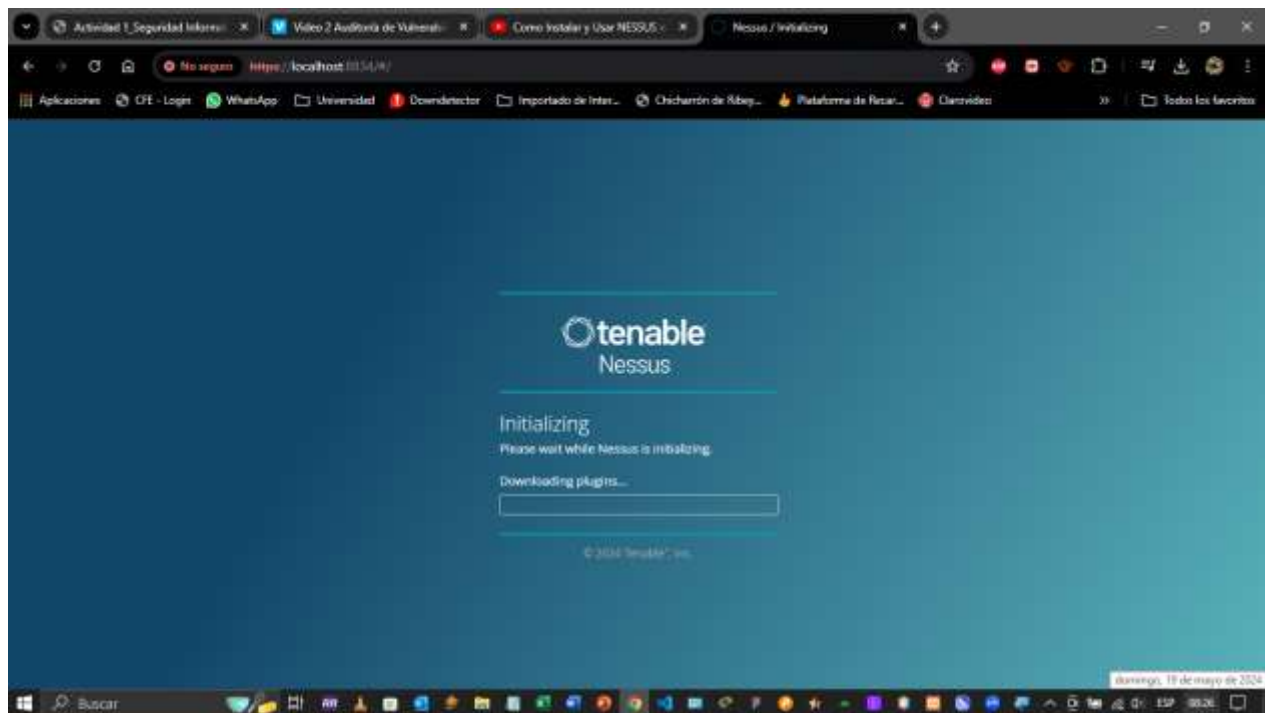




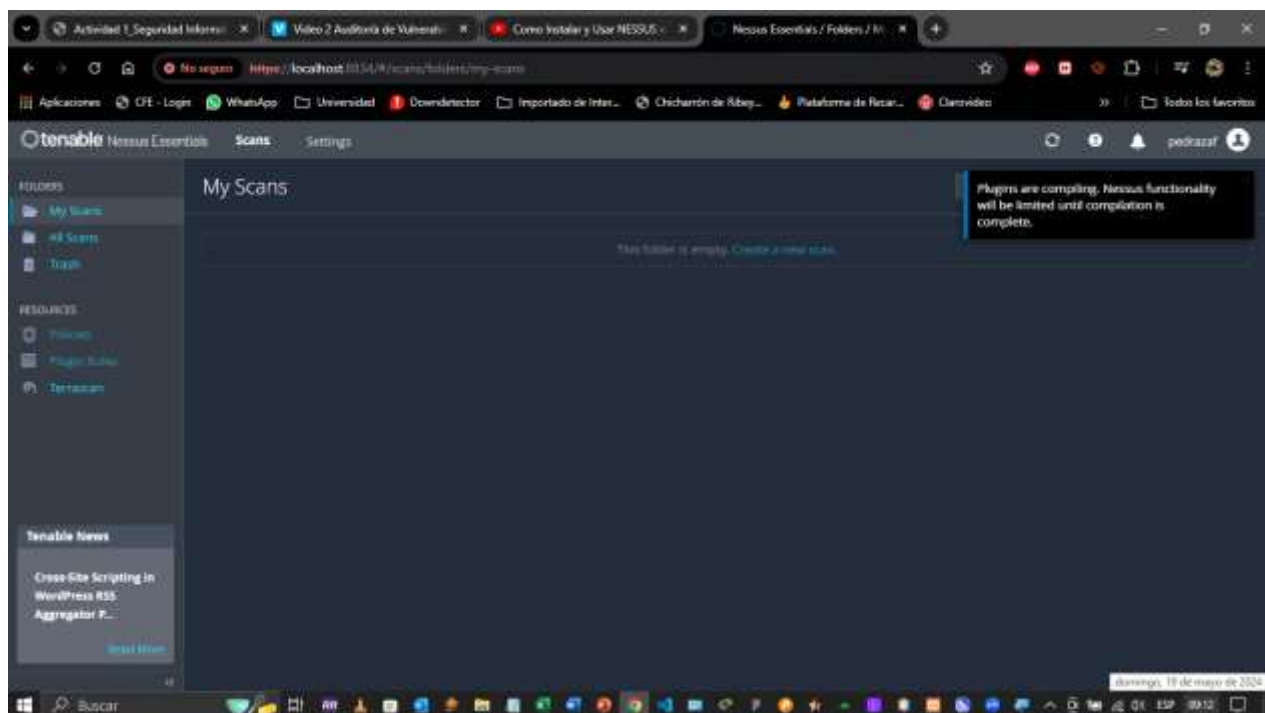
Muestra el código de activación



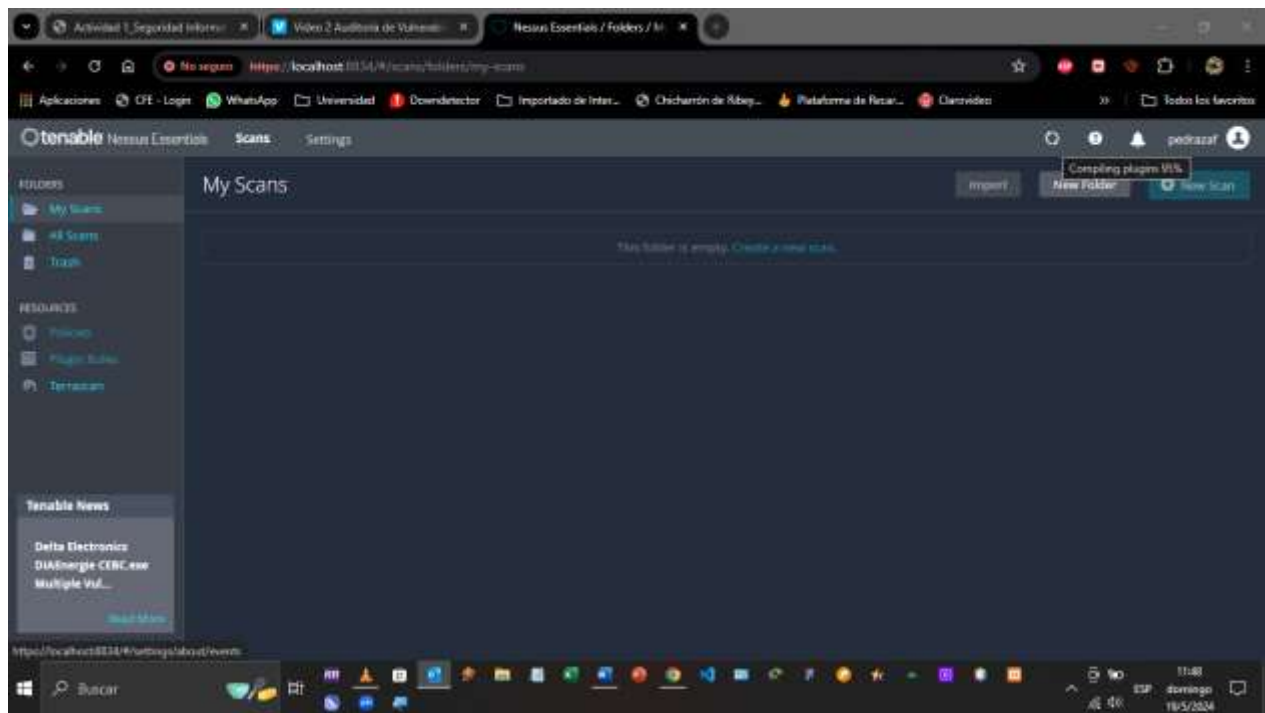
Se crea un usuario y una contraseña robusta



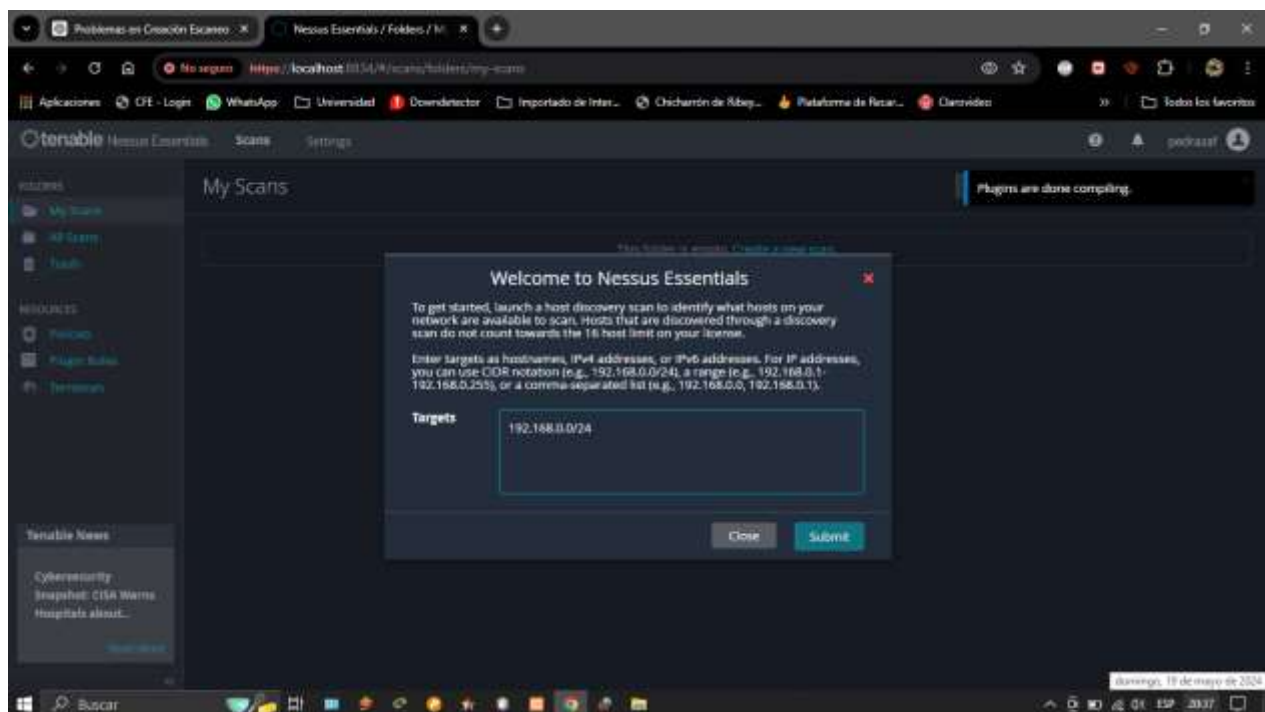
Comienza la instalación

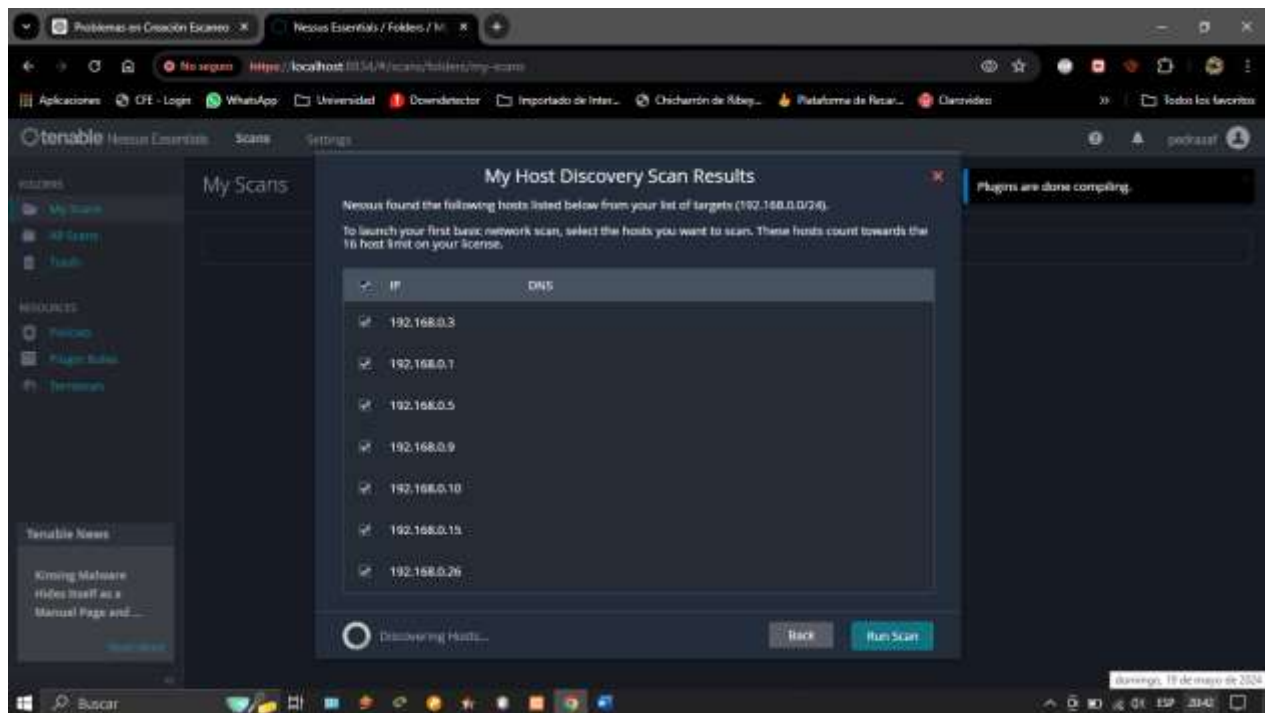


Al concluir se abre la plataforma compilando los plugins para su buen funcionamiento



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





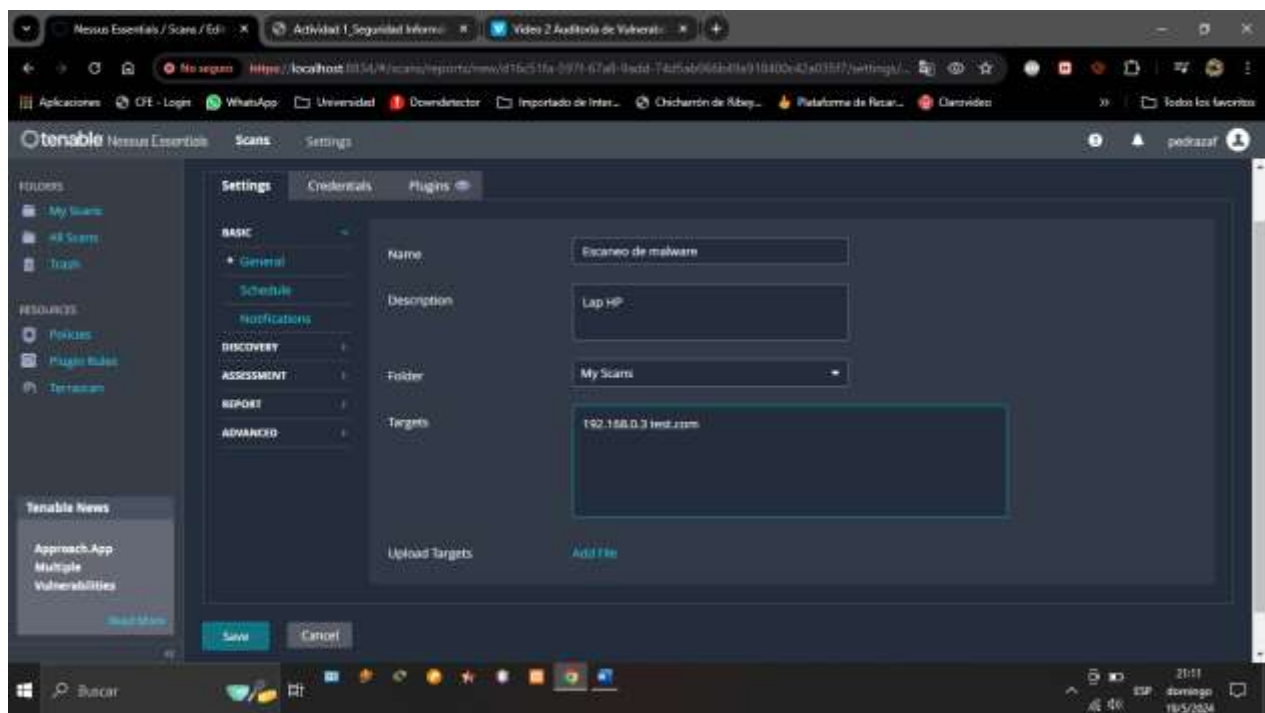
Escaneando los dispositivos que están conectados a la red

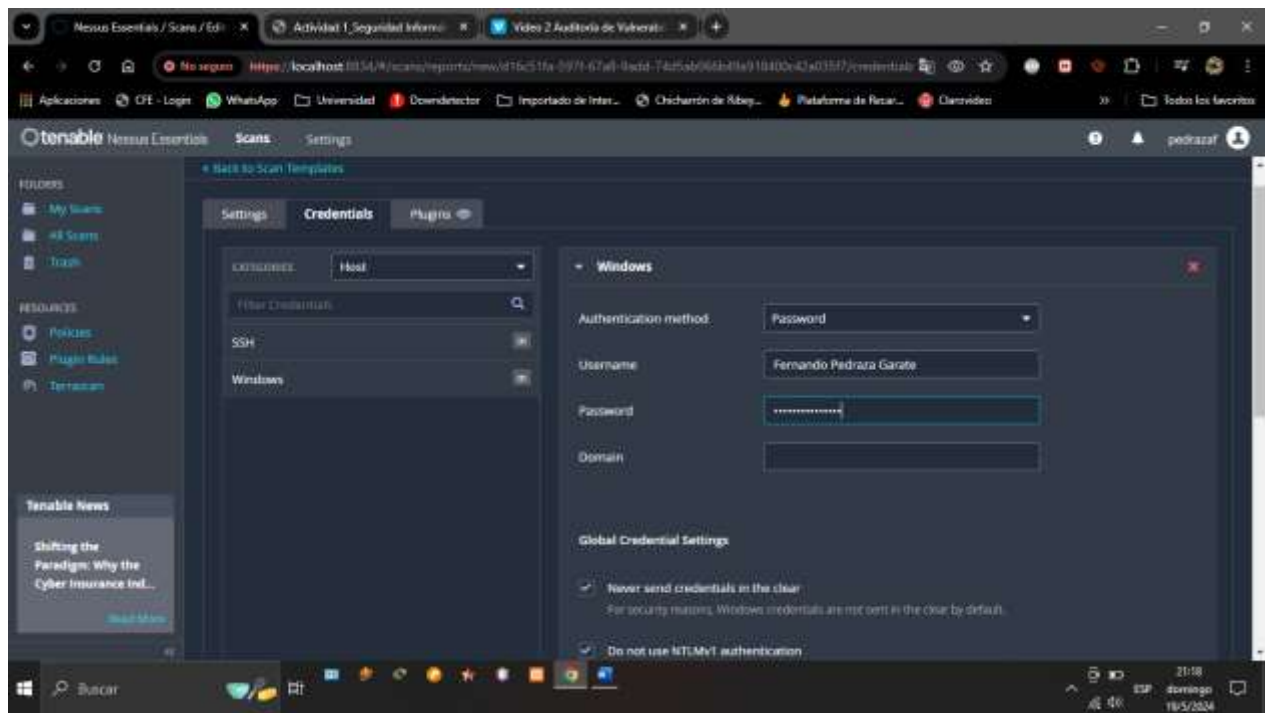


Mostrando el estatus de vulnerabilidad de cada dispositivo conectado a la red

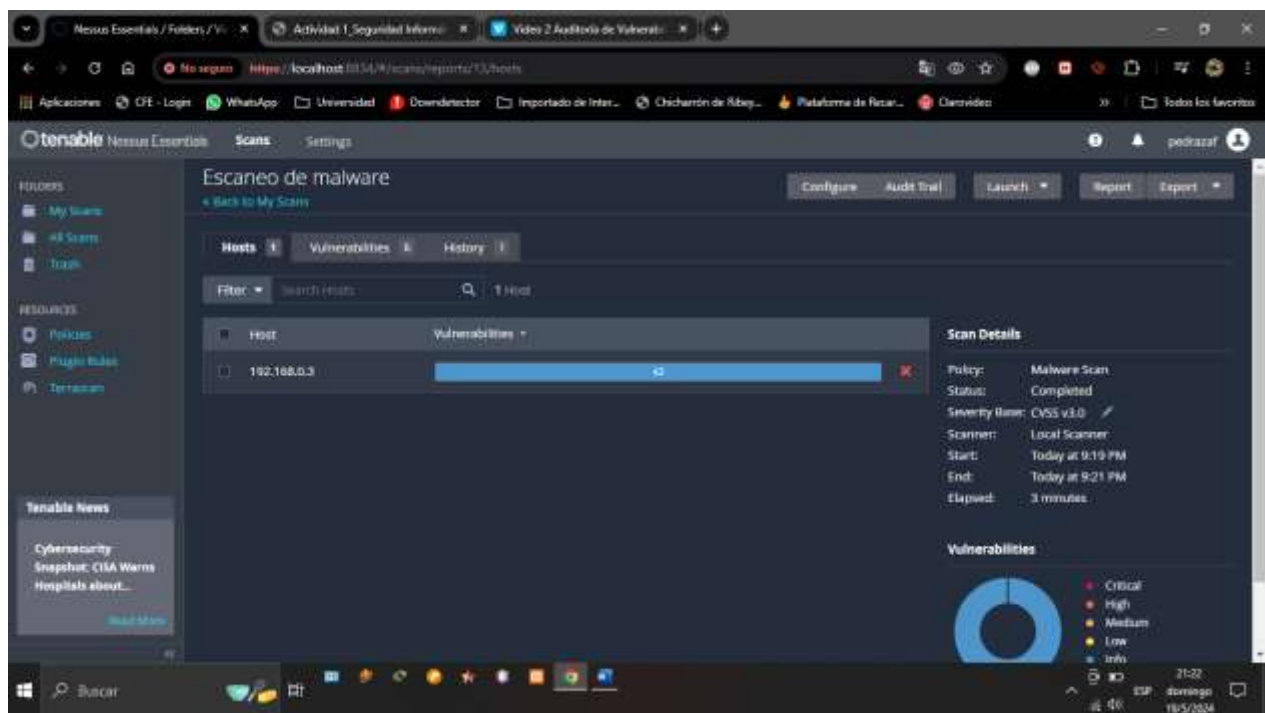


Se crea un nuevo escaneo en busca de malware



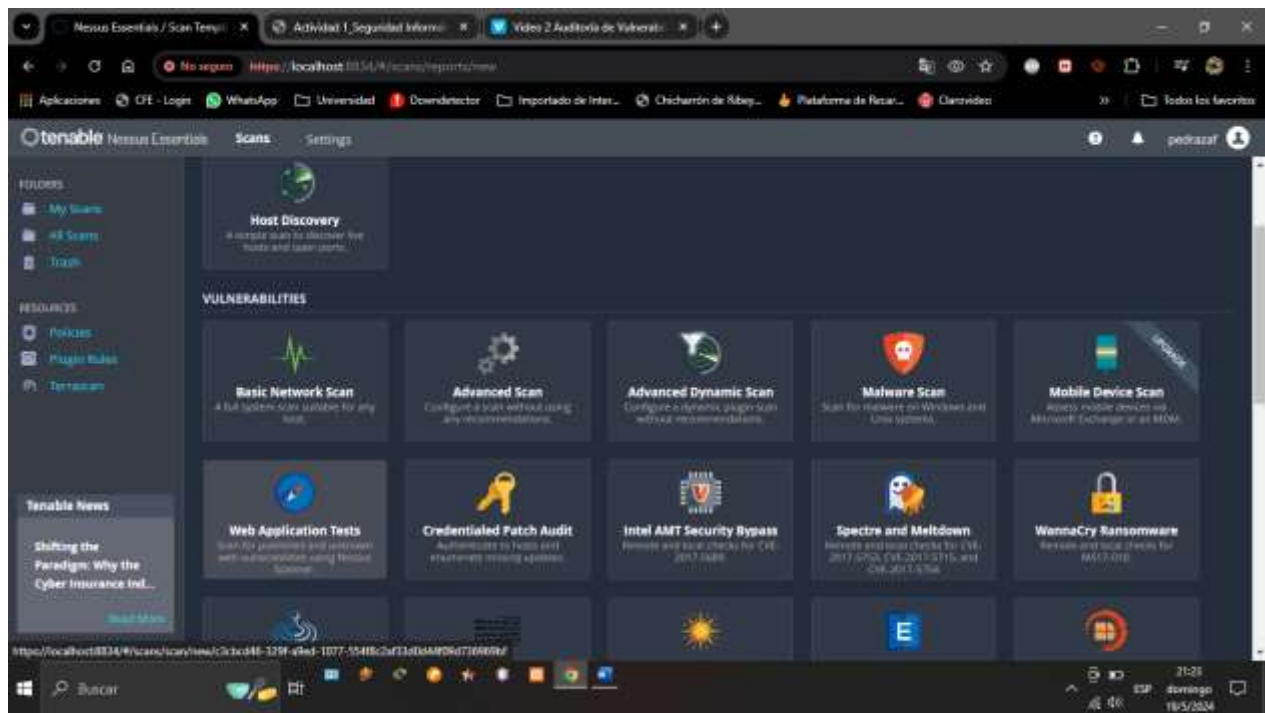


Se ingresan las credenciales y se ejecuta el programa

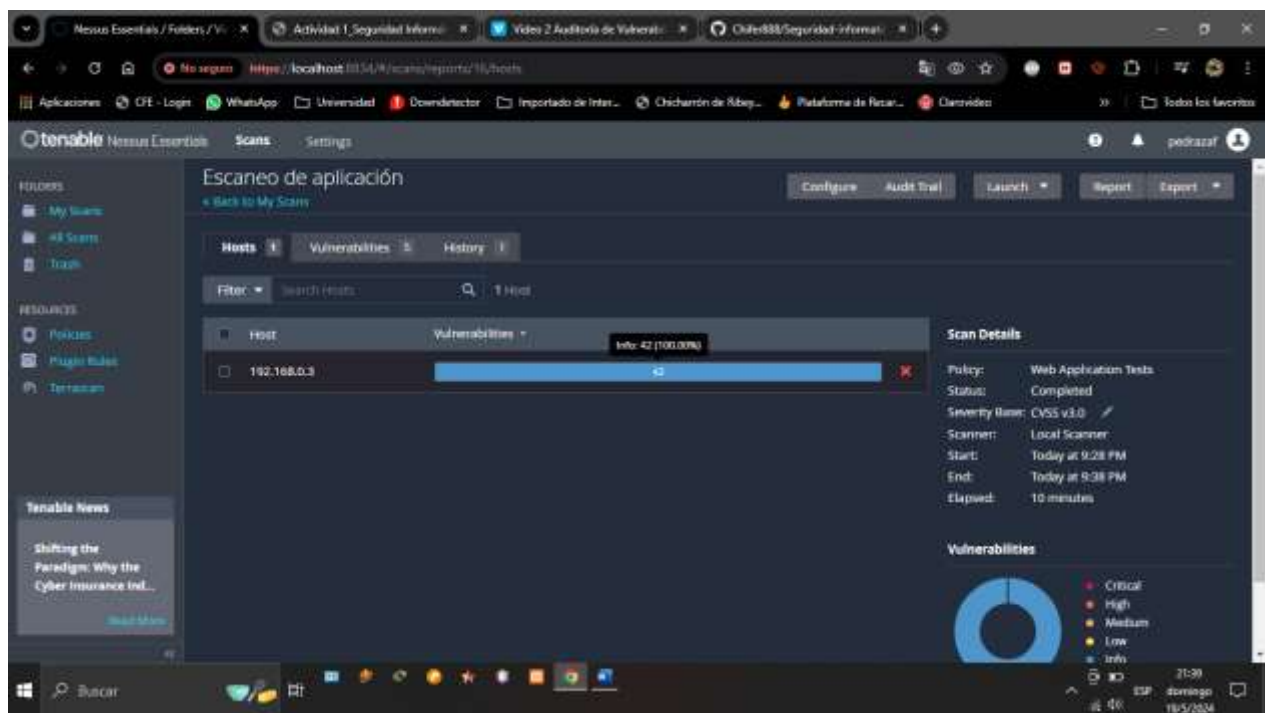


Mostrando los resultados del análisis al terminar el escaneo

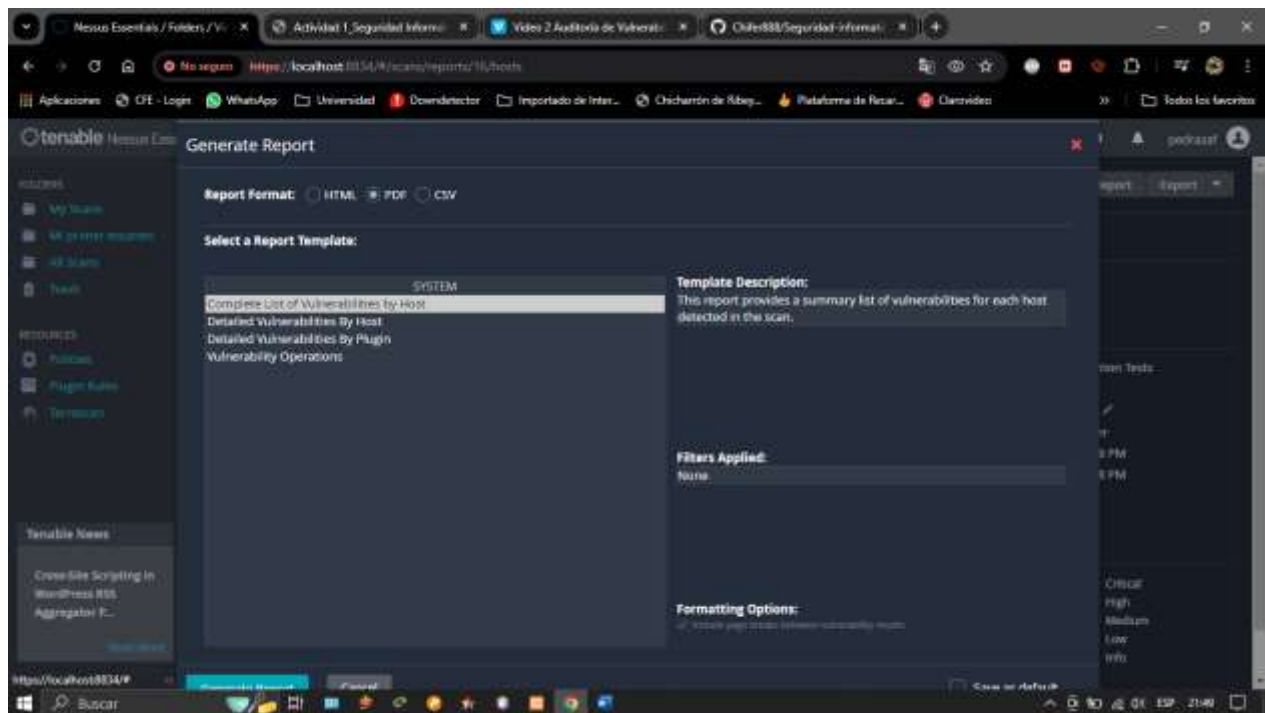




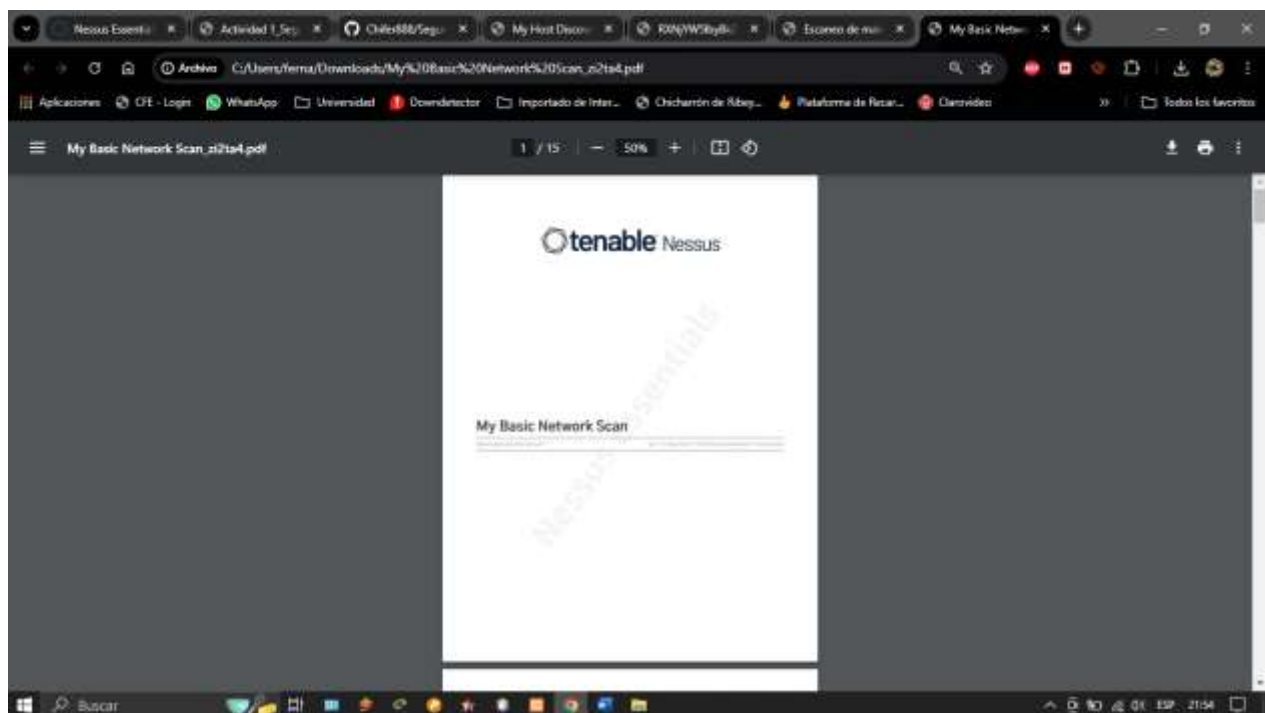
Se crea un escaneo de aplicación web para detectar vulnerabilidades de navegación.



Mostrando los resultados al final del escaneo

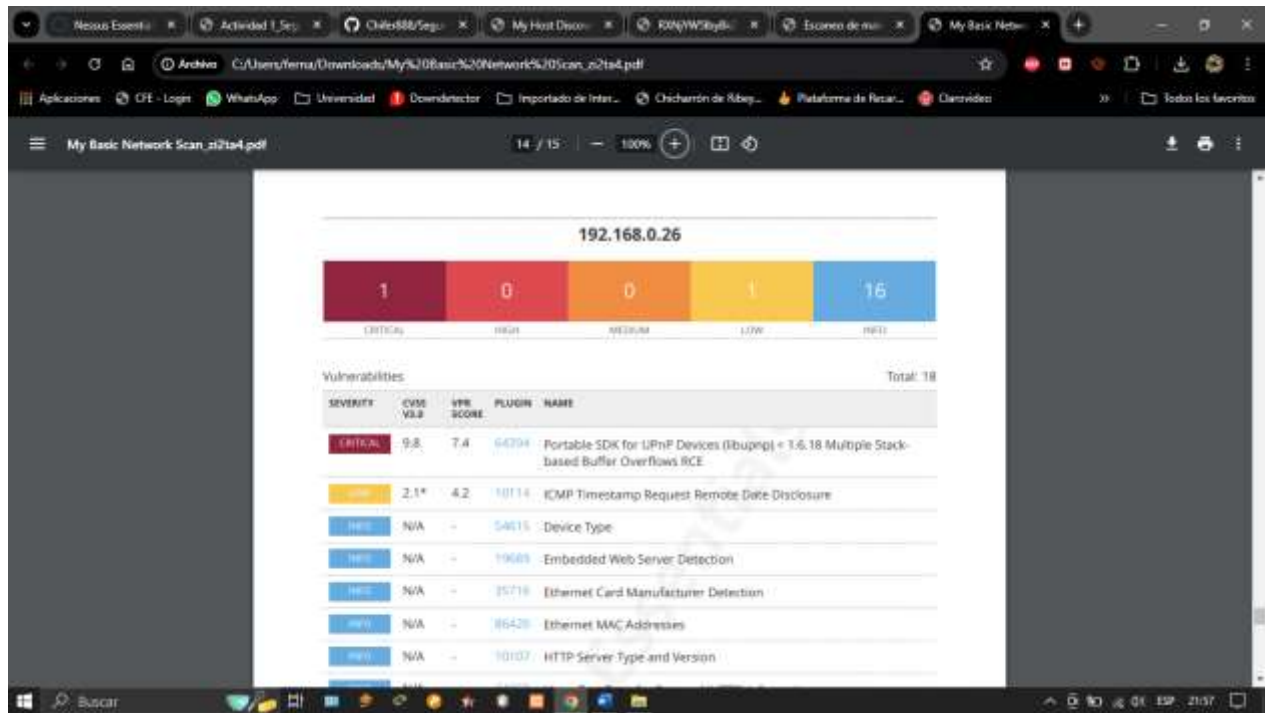


Se crean los reportes en el formato deseado como PDF, HTML o CSV



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





# 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.

¿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.

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>