- Portada
- Índice
- Introducción
- Descripción
- Justificación
- Desarrollo:
- Incidencias encontradas
- Reporte
- Análisis e Identificación de mejoras.
- Conclusión
- Referencia

Actividad [#] 1

[Nombre de la Actividad]Detección y prevención de Ataques de acceso

[Nombre del Curso] Seguridad informática II

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero
Alumno: Daniel Alcudia Almeyda
Fecha:27/05/2023

● Índice

Contenido

● Introducción

La necesidad de la detención de amenazas es tan alta cómo cuál quiere otra protección y protocolo de seguridad. Estos procesos desempeñan un papel esencial para detener los ataques antes de que causen daños irreparables. Al contener las instrucciones maliciosas a tiempo, las empresas pueden mitigar que estos riesgos se filtren a otras áreas de la empresa. Un ataque no contenido puede tener un efecto que puede llegar a paralizar toda una organización esto puede provocar la pérdida de miles o millones de dólares en ventas, clientes y la confianza del público en la marca.

Un beneficio que a menudo se pasa por alto de la detención de amenazas es la importancia que tiene para evitar que los ataques se propaguen a otras áreas de los sistemas y las redes. Este tipo de contención puede ser el factor que determine si una empresa sigue operando o deja de funcionar. También abre oportunidades importantes para actualizar los procesos y procedimientos de prevención, detección, identificación, respuesta y recuperación.

● Descripción

En esta actividad debemos instalar un software que nos permita detectar las vulnerabilidades de nuestro sistema para detectar los factores que puedan implicar los diferentes ataques y así poder prevenirlos antes de que sea demasiado tarde. Para ello debemos instalar la aplicación Nessus la que nos permitirá escanear nuestros dispositivos y poder detectar las posibles fallas de seguridad en nuestros equipos, es decir con Nessus podremos detectar las vulnerabilidades de nuestro sistema.

Con Nessus se pueden escanear los puertos y así poder detectar cuales son lo puertos que se encuentran abiertos, identifica los servicios que utilizan los puertos, compara la información escaneada y la compara con sus bases de datos y señala cuales son las fallas de seguridad, el sistema revisa que no haya dispositivos dentro de los resultados de la investigación.

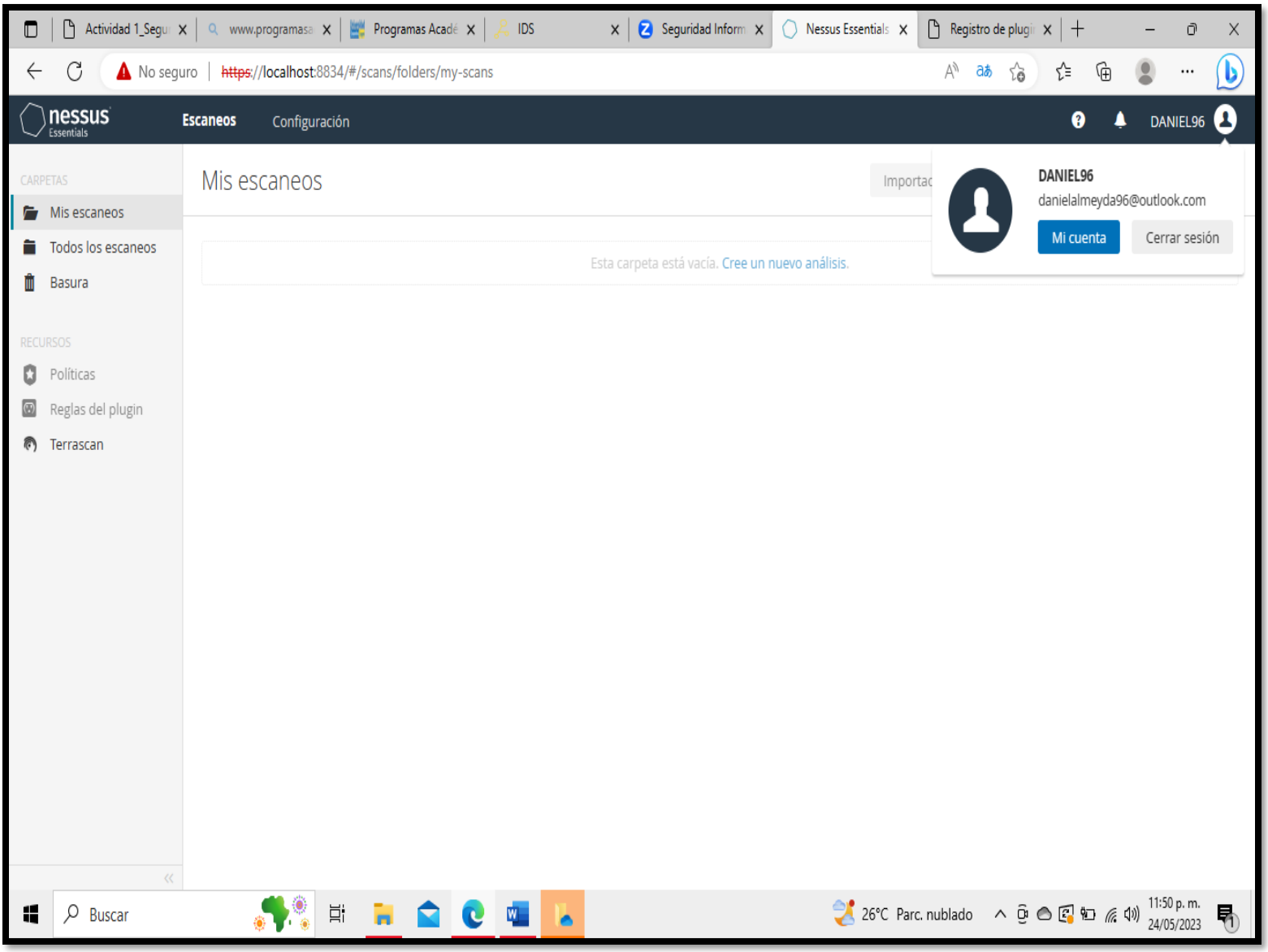
En conclusión, podemos considerar que Nessus es unos de los posibles softwares que nos permite poder detectar las vulnerabilidades de nuestros dispositivos y así poder evitar los posibles ataques que ponga en riesgo nuestra información.

● Justificación

La detención de amenazas es una de las mejores prácticas para mitigar los peligros y las vulnerabilidades como tal la creación de una estrategia para prevenir riesgo es esencial para el éxito a largo plazo de cualquier organización

La detención de amenazas es una de las mejores prácticas para mitigar los peligros y las vulnerabilidades. Cómo tal la creación de una estrategia para prevenir riesgos es esencial para el éxito a largo plazo de cualquier organización. Se ha demostrado que una estrategia eficaz para detectar amenazas conduce a beneficios más allá de los previstos. Los beneficios generales de la detención de amenazas son similares para todas las organizaciones incluyendo ahorro de tiempo, ahorro de dinero, genera confianza en el consumidor, establece la lealtad, minimizar la reparación de la marca, prevención de amenazas, reducción el tiempo de inactividad, proteger la información sensible, mantener el cumplimiento, brindar una mejor atención para ganarse la confianza de los clientes.

- Desarrollo:
- Incidencias encontradas
- Reporte



● Análisis e Identificación de mejoras.

● Conclusión

Todas das por organizaciones que hayan implementado un sistema de gestión de seguridad de la información deberían, por lo menos una vez al año, realizar una auditoría de su ciberseguridad para conocer el estado de protección de sus activos ataques cibernéticos y hacer ajustes.

En conclusión, llevar a cabo una auditoría de ciberseguridad permite a las empresas estar al tanto de posibles fallas, debilidades y errores en un sistema de seguridad y a partir de esto, tomar acciones oportunas para corregirlos y prevenir la materialización de incidentes y ataques cibernéticos que puedan impactar negativamente no sólo la operación normal de la organización, sino también sus finanzas y su reputación. Para prevenir los riesgos asociados a la seguridad de la información y a la ciberseguridad, es importante es gestionar de manera oportuna y adecuada todos los activos de información identificar los diferentes riesgos a los que están expuestos y así prevenir cualquier alerta que pueda presentarse.

● Referencia

Detección y Prevención de Amenazas Informáticas. (2022, septiembre 8). Preyproject.com. https://preyproject.com/es/blog/deteccion-y-prevencion-de-amenazas-su-guia-para-mantenerse-a-salvo

Pirani. (s/f). *Auditoría de ciberseguridad: todo lo que necesitas saber*. Piranirisk.com. Recuperado el 26 de mayo de 2023, de https://www.piranirisk.com/es/academia/especiales/auditoria-de-ciberseguridad-empresas