Instituto Tecnológico y de Estudios Superiores de Monterrey

Inteligencia artificial avanzada para la ciencia de datos I (Gpo 101)

Equipo 4

Cloud computing | Actividad 4 - CIS Benchmarks

Integrantes:

Eliezer Cavazos Rochin A00835194

Facundo Colasurdo Caldironi A01198015

Saul Francisco Vázquez del Río A01198261

José Carlos Sänchez Gómez A01174050

Campus Monterrey **Fecha: 14/10/20**

El CIS Benchmarks son guías de seguridad las cuales son reconocidas a lo largo de la web, desarrolladas por CIS (Center of internet Security), que tienen la utilidad de dejar en claro las configuraciones necesarias de seguridad para poder proteger los sistemas frente a la web, al mismo tiempo, estas guías cubren una amplia gama de tecnologías que se usan día a día, desde sistemas operativos, plataformas de la nube, hasta dispositivos móviles.

Cada uno de estos documentos se encuentra organizado por distintos niveles de seguridad de los mismos, donde mientras más altos sean los niveles, mayor significancia tendrán en los cambios que hacen, a su vez, estos son usados para cumplir con las normas de seguridad internacional, tales como; ISO/IEC 27001, HIPAA y PCI-DSS. Todo lo anterior nos deja en claro que estas guías son esenciales para cualquier organización que busque mejorar su seguridad virtual

Al comparar la configuración de seguridad del sistema operativo analizado con las recomendaciones del CIS Benchmark, se identificaron varias brechas clave que existían en nuestro sistema operativo; La primera de ellas fue la falta de atención a los estándares de complejidad y del cambio de las contraseñas, la cual puede llegar a comprometer la eficacia de las contraseñas a lo largo del tiempo, si no que también incrementa el riesgo de accesos no autorizados.

Otra brecha significativa es la ausencia de cifrado en el disco duro, lo que puede provocar que los datos queden expuestos, lo anterior compromete la confidencialidad de la información. Además, la incorrecta configuración de las actualizaciones automáticas puede resultar en que el sistema esté expuesto a vulnerabilidades que ya han sido solucionadas en versiones más recientes.

Otro punto de interés se vio en el firewall de Windows, aunque se encuentre activado, podría no estar bloqueando todas las conexiones entrantes no solicitadas. Esto podría permitir accesos no autorizados a la red y a recursos internos. Por ello, es crucial revisar las reglas del firewall para garantizar que todas las conexiones no deseadas sean efectivamente bloqueadas. Por último, la falta de un registro de eventos de seguridad adecuado puede resultar en la pérdida de información valiosa sobre intentos de acceso no autorizados o fallos del sistema, dificultando la detección y respuesta ante incidentes de seguridad.

Para mitigar las brechas de seguridad identificadas, se propusieron diversas soluciones para asegurarse que estas fueran eliminadas. Primeramente, se buscó solucionar la política de las contraseñas, recomendando configurar contraseñas de mayor tamaño y complejidad, al mismo tiempo, se incitó a activar el BitLocker para cifrar los datos de los discos duros, como una medida sencilla y efectiva para proteger los datos.

Además, para asegurarnos que el sistema contará con las últimas actualizaciones, se habilitaron las actualizaciones automáticas del sistema, también,

se puso especial cuidado en el firewall de Windows, el cual fue designado para estar activo en todos los perfiles, finalmente, se decidió habilitar el registro de eventos de seguridad, ya que es esencial para monitorear incidentes y posibles ataques.

Durante el análisis del sistema operativo, se observó que el equipo cuenta con configuraciones necesarias para garantizar una cuenta segura y contraseñas complejas, lo que mejora significativamente la seguridad. Además, se verificó que el firewall de Windows está activado, bloqueando las conexiones entrantes no deseadas.

El Sistema operativo también tiene las actualizaciones automáticas habilitadas, asegurando que esté al día con las últimas mejoras de seguridad. Asimismo, se confirmó que Windows Defender está activado y actualizado para brindar protección contra malware. Por último, se observó que el navegador web está protegido, ofreciendo seguridad frente a sitios maliciosos y controlando la información que estos sitios pueden obtener.

En conclusión, la implementación de las recomendaciones del CIS Benchmarking son fundamentales para no solo fortalecer la seguridad de los sistemas operativos, sino también, para prevenir las posibilidades de ataques realizadas por los terceros, más, es necesario asegurarse que estas estén implementadas de manera correcta, como la mejora en la política de contraseñas, la activación del cifrado de disco, la correcta configuración de actualizaciones automáticas y la supervisión mediante registros de eventos de seguridad, ya que ayudan a generar un espacio seguro de trabajo, y también a cumplir con normativas internaciones de seguridad