Instituto Tecnológico y de Estudios Superiores de Monterrey
Campus Monterrey

Inteligencia artificial avanzada para la ciencia de datos II
TC3007C, Grupo 101

Nombre del profesor: Félix Ricardo Botello Urrutia

Cloud computing | Actividad 4 - CIS Benchmarks

Equipo 6 | Integrantes:

Oskar Arturo Gamboa Reyes	| A01173648
Ricardo Salinas	| A01284657
Oscar Gutiérrez Araiza	| A00832992
Erika Martínez	| A01028621
Marcelo de Luna	| A00832239

Octubre 2024

1. Sistema Operativo

MacOs Sequoia

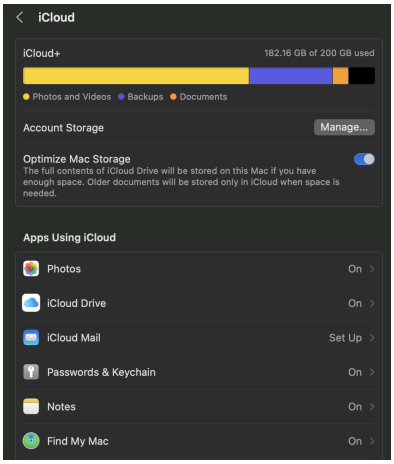
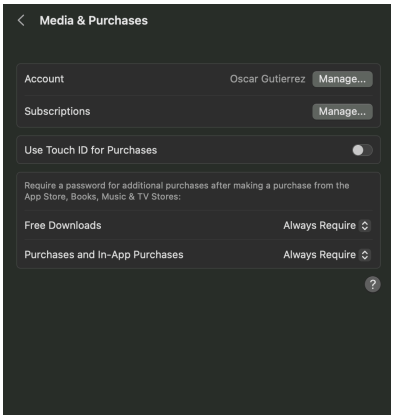
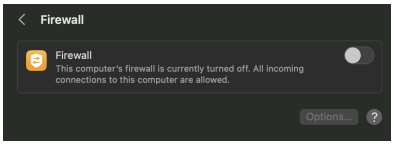
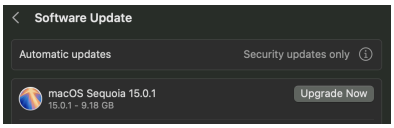
2. En base a ese SO seleccionado, buscar un Benchmark en el portal del CIS con el que trabajarán en lo siguiente:
    - Analizar el Benchmark seleccionado, sus políticas de hardening y configuración.
    - Comparar dichas políticas del Benchmark con la configuración del SO del equipo seleccionado.
    - Identificar las posibles brechas de seguridad del equipo, en base a lo recomendado en el Benchmark.

16.7 Use Standard Hardening Configuration Templates for Application Infrastructure Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.

3. Realizar un informe de cumplimiento que incluya una evaluación detallada de las configuraciones de seguridad existentes y una descripción de las acciones recomendadas para cumplir con las mejores prácticas de CIS Benchmarks.

4. Proporcionar recomendaciones prácticas y factibles para implementar las mejoras de seguridad identificadas, teniendo en cuenta los recursos y las limitaciones organizacionales.

Configuración	Recomendación	Posible brecha de seguridad

	2.1.1.6 Audit Find My Mac (Manual) Deshabilitar Find My, no es una solución destinada para empresas.	Alguna persona no deseada puede acceder a la ubicación en tiempo real del dispositivo.
	2.1.2 Audit App Store Password Settings (Manual) Asegurarse de que la contraseña siempre sea requerida para realizar descargas o compras.	Si la contraseña no siempre es requerida, alguien no autorizado podría realizar compras o descargas.
	2.2.1 Ensure Firewall Is Enabled (Automated) Verificar que el firewall esté encendido.	El sistema queda vulnerable a accesos no autorizados, ataques externos y malware.
	2.3.1.1 Ensure AirDrop Is Disabled When Not Actively Transferring Files (Automated) Asegurarse de que AirDrop está desactivado cuando no se está utilizando.	Tener airdrop activado cuando no se está utilizando permite que se hagan requests para enviar contenido no deseado. También permite que dispositivos en la red local encuentren la laptop por medio de bluetooth.
	1.1 Ensure All Apple-provided Software Is Current (Automated)	Al no tener actualizaciones automáticas, los agentes maliciosos pueden aprovechar

	Asegurarse de tener las actualizaciones automáticas.	vulnerabilidades que hayan sido descubiertas.

Importancia de Configuración

Mantener un sistema operativo actualizado puede disminuir la probabilidad de ataques cibernéticos, virus y malware, esto demuestra la importancia de mantener las configuraciones relacionadas con la seguridad al día. Además, muchas actualizaciones no solo corrigen fallos de seguridad, sino que también mejoran el rendimiento y estabilidad del sistema, lo que contribuye a un mejor funcionamiento en general. Ignorar estas actualizaciones puede dejar abierta la puerta a vulnerabilidades que ya han sido identificadas y que los hackers aprovechan rápidamente. Por eso, no solo se trata de tener el software más reciente, sino de asegurarse de que cada componente esté optimizado para prevenir cualquier posible riesgo.

Hallazgos

A lo largo de esta comparación entre el sistema operativo actual y el benchmark, pudimos ver que muchas de las recomendaciones de seguridad del sistema no se cumplían, lo cual nos permitió realizar las correcciones necesarias y analizar a fondo el impacto que puede tener la falta de estas medidas preventivas en la seguridad de la computadora. Al identificar estas deficiencias, logramos no solo mejorar la configuración, sino también prevenir posibles riesgos que podrían comprometer la integridad del sistema y los datos almacenados.

Conclusión

En general, la seguridad de una computadora depende en gran medida de su sistema operativo y de cómo se configuren sus opciones de seguridad. Existen diversos tipos de amenazas que pueden afectar la seguridad y privacidad del usuario, lo que hace crucial seguir las regulaciones y buenas prácticas establecidas en el benchmark correspondiente al sistema operativo. Al cumplir con estas normativas, no solo se refuerza la protección del sistema, sino que también se minimizan los riesgos de vulnerabilidades que podrían ser explotadas por ataques externos.

Referencia

Center for Internet Security. (2024). *CIS Apple macOS 13.0 Ventura Benchmark* (v2.1.0). https://www.cisecurity.org