

Campus Monterrey

Materia

Inteligencia artificial avanzada para la ciencia de datos II

Tarea

Cloud computing | Actividad 4 - CIS Benchmarks

Estudiantes

Cleber Gerardo Pérez Galicia - A01236390

Juan Pablo Bernal Lafarga - A01742342

Jacobo Hirsch Rodríguez - A00829679

Eryk Elizondo González - A01284899

Profesor

Félix Ricardo Botello Urrutia

Las CIS Benchmarks son recomendaciones de configuración prescriptivas para más de 25 familias de productos de proveedores. Representan el esfuerzo basado en el consenso de expertos en ciberseguridad a nivel mundial para ayudar a proteger sus sistemas contra amenazas con mayor confianza.

Entre las benchmarks disponibles, se incluyen de proveedores de nube como GCP, Azure, AWS; dispositivos móviles como Android y IOS; sistemas operativos como Linux, macOS, windows, entre muchos otros.

Análisis de Configuración de Benchmark

Sistema Operativo Elegido: Windows 11 Stand-alone

Security Options

1. 2.3.1 Accounts




Recomendación

2.3.1.4 (L1) Configure 'Accounts: Rename administrator account'

Descripción

La cuenta local default de administrador tiene un nombre de cuenta conocido que los atacantes buscarán atacar. Se recomienda elegir otro nombre para esta cuenta que no tenga relación con un rol administrativo.

Configuración en el Sistema Operativo

 Default	6/19/2024 10:16 PM	File folder
 eryke	10/3/2024 2:12 PM	File folder
 Public	6/19/2024 9:16 PM	File folder

Actualmente el nombre de la cuenta de administrador es diferente al default con el nombre de eryke.

Acciones Recomendadas

Como la cuenta de administrador local posee un nombre distinto al default, la configuración del sistema operativo ya cumple con las mejores prácticas para este punto.

2. 2.3.1 Accounts




Recomendación

2.3.1.2 (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled'

Descripción

La cuenta local default de invitado permite a usuarios no autenticados acceso a la red del sistema.

Configuración en el Sistema Operativo

 Default	6/19/2024 10:16 PM	File folder
 eryke	10/3/2024 2:12 PM	File folder
 Public	6/19/2024 9:16 PM	File folder

Actualmente la cuenta de invitado se encuentra activa.

Acciones Recomendadas

Se recomienda deshabilitar y renombrar la cuenta de invitado para cumplir con las mejores prácticas para este punto.

3. 2.3.11 Network security





















Recomendación

2.3.11.2 (L1) Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'

Descripción

Esta configuración de política determina si NTLM puede recurrir a una sesión NULL cuando se utiliza con LocalSystem.

Configuración en el Sistema Operativo

Name
 (Default)
 auditbasedirectories
 auditbaseobjects
 Authentication Packages
 Bounds
 crashonauditfail
 disabledomaincreds
 everyoneincludesanonymous
 forceguest
 fullprivilegeauditing
 LimitBlankPasswordUse
 LsaPid
 NoLmHash
 Notification Packages
 ProductType
 restrictanonymous
 restrictanonymoussam
 SamConnectedAccountsExist
 SecureBoot
 Security Packages

Actualmente no existe una configuración de Allow LocalSystem NULL session fallback.

Acciones Recomendadas

Se recomienda agregar la variable en el registry y deshabilitar la opción para cumplir con las mejores prácticas para este punto.

Windows Defender Firewall with Advanced Security

4. 9.2 Private Profile


Recomendación

9.2.1 (L1) Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'

Descripción

Seleccione Activado (recomendado) para que Windows Firewall con Seguridad Avanzada utilice la configuración de este perfil para filtrar el tráfico de red. Si selecciona Desactivado, el Firewall de Windows con Advanced Security no utilizará ninguna de las reglas de firewall o reglas de seguridad de conexión para este perfil.

Configuración en el Sistema Operativo

 Private networks Not connected ^	
Networks at home or work where you know and trust the people and devices on the network	
Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	None
Notification state:	Notify me when Windows Defender Firewall blocks a new app

La configuración del sistema operativo ya sigue las mejores prácticas para este punto.

Acciones Recomendadas

Como se encuentra activado la configuración de firewall para perfiles privados, la configuración del sistema operativo ya cumple con las mejores prácticas para este punto.

5. 9.3 Public Profile

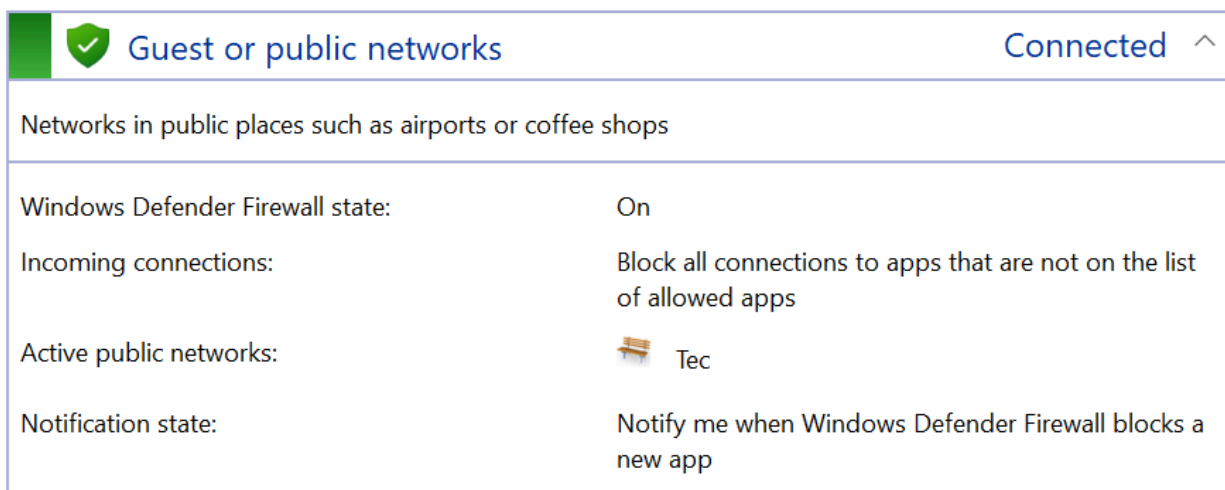
Recomendación

9.3.1 (L1) Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'

Descripción

Seleccione Activado (recomendado) para que Windows Firewall con Seguridad Avanzada utilice la configuración de este perfil para filtrar el tráfico de red. Si selecciona Desactivado, el Firewall de Windows con Advanced Security no utilizará ninguna de las reglas de firewall o reglas de seguridad de conexión para este perfil.

Configuración en el Sistema Operativo



La configuración del sistema operativo ya sigue las mejores prácticas para este punto.

Acciones Recomendadas

Como se encuentra activado la configuración de firewall para perfiles públicos, la configuración del sistema operativo ya cumple con las mejores prácticas para este punto.

Referencias Bibliográficas

- CIS. (s.f.). CIS Benchmarks List. *Center for Internet Security*. Recuperado de:
<https://www.cisecurity.org/cis-benchmarks>