	HARDENING MYSQL	
		V.1

CONTROL DE VERSIONES

Elaborado por:	Haranklob Ocampo y Juan Saldarriaga	**No. de Versión:**	1
Revisado por:		**Fecha de revisión:**	
Aprobado por:		**Fecha de aprobación:**	

Historia de Modificaciones

No. de Versión	Fecha de Versión	Autor	Revisado por	Aprobado por	Descripción
1	Febrero 24, 2023	Haranklob Ocampo y Juan Saldarriaga			

1. DESCRIPCIÓN GENERAL

Objetivo

Presentar los puntos primordiales para ejecutar un proceso de gestión de seguridad y auditoria de los servicios del motor de Base de Datos MySQL, establecidos por SETI, basados en documentos generados por el Fabricante y en la experiencia de SETI S.A.S.

Definiciones

Observaciones

Este documento está elaborado de tal forma que puede ser aplicado a la versión 8.0 del motor de base de datos MySQL.

Tener en cuenta:

- Los Hardening por demanda realizados por parte del cliente pueden generar oportunidades de mejora puesto que los servicios están en constante cambio o evolución.
- Cualquier punto tratado en este documento podría representar un Riesgo el cual demandará un análisis más profundo del tema específico.
- La ejecución de esta actividad de Hardening puede llevar a la planeación y ejecución de actividades de PAYM.

Las tareas presentadas en este documento también aplican cuando se desea ajustar y mejorar los lineamientos vigentes conforme lo demanden las buenas prácticas del fabricante o la experiencia de SETI.

La Plantillas Default mencionada en este documento, se relacionan a continuación:
CIS_Oracle_MySQL_Enterprise_Edition_8.0_Benchmark_v1.1.0.pdf

CALIFICACION GENERAL DEL HARDENING

Teniendo en cuenta los puntos tratados en este documento , su nivel de criticidad y las evidencias obtenidas , resultado del proceso ejecutado, se presenta a continuación una tabla con los hallazgos que permitirá calificar el nivel de cumplimiento de este Hardening.

		NO CUMPLIMIENTO DE VULNERABILIDADES		
CAPA		**ALTA**	**MEDIA**	**BAJA**
BASES DE DATOS	**VULNERABILIDADES**	**##%**	**##%**	**##%**
	Sistema Operativo			
	Log de Instancia			
	Archivos de Configuración			
	TableSpace			
	Roles, Usuarios y Permisos			
	Consideraciones especiales			
Total ítems Evaluados:	**##**	**#**	**#**	**#**

1. VULNERABILIDADES A NIVEL DE SISTEMA OPERATIVO

TAREA	CRITICIDAD
1. Instalación y Parches: **DESCRIPCIÓN:** Se deben verificar que se cuente con las últimas versiones liberadas por el Fabricante, es necesario determinar que los parches se hayan obtenido de repositorios autorizados y confiables, según manual del fabricante. **NOTA:** Si se utilizan repositorios no autorizados o confiables se corre el riesgo de utilizar productos manipulados por terceros, con altas fallas de seguridad o rastreo, incluso, sin ningún tipo de documentación de soporte valida. **AUDITORIA:** A. Asegure que las versiones de los paquetes principales coincidan todas con la versión actual del producto: `SELECT version();` **EVIDENCIAS:**	**Alta**
2. Conexión Directa con Usuario "mysql" a Nivel de SO: **DESCRIPCIÓN:** Este usuario es comúnmente conocido por ser el propietario del servicio e instalación de los motores MySQL, por lo que es buscado para hacer intrusión directa a las bases de datos con permisos de Super Administrador. Se hace necesario establecer las siguientes pautas para controlar su uso, teniendo en cuenta que solo los consultores pertenecientes al grupo DBA deben contar con acceso al Motor de forma directa mediante el Sistema Operativo: ➢ Crear usuarios nombrados ya sea para SETI o para cada consultor perteneciente al grupo DBA. ➢ Otorgar permisos a los usuarios anteriores para hacer SUDO hacia el usuario "mysql". ➢ Activar, mediante el usuario root, el registro o seguimiento de todas las actividades ejecutadas tanto por los usuarios nombrados como por el usuario "mysql". ➢ Establecer procesos de auditoría de la información de rastreo o seguimiento (directamente por el área encargada en el cliente) de las labores ejecutadas por el usuario "mysql", así, como los intentos correctos	**Alta**

TAREA	CRITICIDAD

y fallidos de SUDO a este usuario o de conexión al Sistema Operativo, para monitorear el uso de usuarios y permisos, además, de visualizar eventos de acceso indebido.
 	
NOTA: El no asegurar el acceso al usuario "mysql" pone en grave riesgo la información y vida útil de los datos almacenados en las Bases de Datos de la Instancia de MySQL.
AUDITORIA:
A. Visualizar la lista de usuarios con permisos de SUDO:
`getent group sudo`
B. Determinar si el usuario con el cual se ha conectado tiene permisos de SUDO:
`sudo -l`
C. Verificar la asignación de SUDO y permisos para un usuario especifico:
`sudo -l -U user_name`
 	
EVIDENCIAS:	

2. VULNERABILIDADES

TAREA	CRITICIDAD
1. Colocar bases de datos en particiones que no son del sistema: **DESCRIPCIÓN:** Se acepta generalmente que los sistemas operativos host deben incluir sistemas de archivos diferentes particiones para diferentes propósitos. Un conjunto de sistemas de archivos se llama típicamente particiones del sistema, y generalmente se reservan para el funcionamiento del sistema host/aplicación. El otro conjunto de los sistemas de archivos se denomina normalmente "particiones que no son del sistema", y tales ubicaciones son generalmente reservado para almacenar datos. **NOTA:** Aplicable a MySQL RDBMS en Linux.	**Media**

TAREA	CRITICIDAD

Al mover la base de datos fuera de la partición del sistema se reducirá la probabilidad de denegación de servicio causado por el agotamiento del espacio disponible en disco para el sistema operativo.
 	
Mover archivos y directorios de base de datos a una partición que no sea del sistema puede resultar difícil en función de sobre si había una sola partición cuando se configuró el sistema operativo y si hay particiones adicionales no del sistema disponibles.
 	
AUDITORIA:
A. Obtener la ubicación del datadir y otros archivos de base de datos MySQL ejecutando la siguiente consulta:
`SELECT VARIABLE_NAME, VARIABLE_VALUE FROM performance_schema.global_variables WHERE (VARIABLE_NAME LIKE '%dir' or VARIABLE_NAME LIKE '%file') and (VARIABLE_NAME NOT LIKE '%core%' AND VARIABLE_NAME <> 'local_infile' AND VARIABLE_NAME <> 'relay_log_info_file') order by VARIABLE_NAME;`
 	
B. Utilizando el valor devuelto para el datadir, y otros resultados de la consulta anterior, ejecute lo siguiente en un terminal del sistema:
`df -h <directory>`
 	
La salida devuelta por el comando df anterior no debe incluir root (/), /var, o /usr.
 	
SOLUCIÓN: Realice los siguientes pasos para remediar esta configuración para el datadir:
 	
A. Realice una copia de seguridad de la base de datos.
 	
B. Elija una partición que no sea del sistema *(Nueva ubicación)* para los datos de MySQL.
 	
C. Detenga mysqld usando un comando como: `service mysql stop`.
 	
D. Copie los datos usando un comando como: `cp -rp <valor datadir> <nueva ubicación>`.	

TAREA	CRITICIDAD

E. Defina la la nueva ubicación del *datadir* en el archivo de configuración de MySQL.
 	
F. Inicie mysqld usando un comando como: `service mysql start`.
 	
Nota: En algunas distribuciones de Linux es posible que necesite modificar adicionalmente la configuración del *apparmor*. Por ejemplo, en un sistema Ubuntu 14.04.1, edite el archivo */etc/apparmor.d/usr.sbin.mysqld* para que el *datadir* sea el apropiado. El original podría verse así:
 	
`# Allow data dir access`
`/var/lib/mysql/ r,`
`/var/lib/mysql/** rwk,`
 	
Altere esas dos rutas para que apunten a la nueva ubicación que eligió arriba. Por ejemplo, si la nueva ubicación era */media/mysql* y, el archivo /etc/apparmor.d/usr.sbin.mysqld debe incluir algo como esto:
 	
`# Allow data dir access`
`/media/mysql/ r,`
`/media/mysql/** rwk,`
 	
EVIDENCIAS:	

2. <u>Usar una cuenta dedicada con privilegios mínimos para el servicio de MySQL:</u> **DESCRIPCIÓN:** Como cualquier servicio instalado en un host, se le puede proporcionar su propio usuario. Proporcionar un usuario dedicado al servicio proporciona la capacidad de restringir con precisión el servicio dentro del contexto más amplio del host. **NOTA:** Aplicable a MySQL RDBMS en Linux. Utilizar una cuenta con privilegios mínimos para que MySQL se ejecute según sea necesario puede reducir el	**Alta**

TAREA	CRITICIDAD

impacto de una vulnerabilidad nacida en MySQL. Una cuenta restringida no podrá acceder a recursos no relacionados con MySQL, como las configuraciones del sistema operativo.
AUDITORIA: Ejecute el siguiente comando en un terminal del sistema para evaluar esta recomendación:
 	
`ps -ef | egrep "^mysql.*$"`
 	
Si no se devuelve ninguna línea, esto es un error.
 	
NOTA: Se asume que el usuario de MySQL es mysql. Además, puede considerar la posibilidad de ejecutar `sudo -l` como usuario de MySQL o comprobar el archivo sudoers.
 	
SOLUCIÓN: Cree un usuario que sólo se utilice para ejecutar MySQL y procesos directamente relacionados. Este usuario no debe tener permisos administrativos en el sistema. Además, es mejor evitar proporcionar acceso mediante shell a dicha cuenta.
 	
El acceso al shell se puede quitar utilizando el siguiente comando en un terminal del sistema:
 	
`/usr/sbin/groupadd -g 27 -o -r mysql >/dev/null 2>&1 || :`
`/usr/sbin/useradd -M -N -g mysql -o -r -d /var/lib/mysql -s /bin/false \`
`-c "MySQL Server" -u 27 mysql >/dev/null 2>&1 || :`
 	
NOTA: El usuario root puede ser usado para iniciar el servicio MySQL en Linux/UNIX, pero entonces debe ser configurado para quitar privilegios indicando el usuario específico del servicio en my.cnf o my.ini archivo.
 	
EVIDENCIAS:	

3. <u>Deshabilitar el historial de comandos de MySQL:</u> **DESCRIPCIÓN:** En Linux/UNIX, el cliente MySQL y las instrucciones de registro de MySQL Shell se ejecutan interactivamente en un archivo de historial. El archivo de cliente MySQL predeterminado se denomina *.mysql_history* en el directorio de inicio del usuario. Los archivos se dividen por idioma y se denominan	**Alta**

TAREA	CRITICIDAD

history.sql, history.js y *history.py*. La mayoría de los comandos interactivos que se ejecutan en la aplicación cliente MySQL se guardan en un archivo de historial. El historial de comandos de MySQL debe estar deshabilitado. De forma predeterminada, MySQL Shell no guarda el historial entre sesiones.
 	
NOTA: Aplicable a MySQL RDBMS en Linux.
 	
La desactivación del cliente MySQL y el historial de comandos de MySQL Shell reduce la probabilidad de exponer información confidencial, como contraseñas, claves de cifrado u otros datos o información confidenciales.
 	
AUDITORIA: Ejecute los siguientes comandos para evaluar esta recomendación:
 	
`find /home -name ".mysql_history"`
`find /root -name ".mysql_history"`
 	
Para MySQL Shell
 	
`ls -d .??*/* | egrep history | grep mysql`
 	
Para cada archivo devuelto, determine si ese archivo está vinculado simbólicamente a `/dev/null`.
 	
SOLUCIÓN: Para MySQL Client realice los siguientes pasos para corregir esta configuración:
 	
A. Quite .mysql_history si existe.
 	
B. Utilice cualquiera de las siguientes técnicas para evitar que se vuelva a crear:
 	
- Establezca la variable de entorno *MYSQL_HISTFILE* en */dev/null*. Esto deberá colocarse en el script de inicio del shell.
- Cree *$HOME/.mysql_history* como símbolo para */dev/null*.	

TAREA	CRITICIDAD
`> ln -s /dev/null $HOME/.mysql_history` Además, otra forma de evitar que se registre el historial es usar la opción `--batch`. Para MySQL Shell, realice los siguientes pasos para corregir esta configuración: A. Elimine `$HOME/.mysqlsh/history.*` si existen archivos. B. Utilice cualquiera de las siguientes técnicas para evitar que se vuelva a crear: - Iniciar shell y mostrar la lista de opciones mediante `\option -l` - Inhabilite el historial utilizando el comando `\option -persist history.autoSave=1` **VALOR POR DEFECTO:** Por defecto, el archivo de historial de comandos de MySQL se encuentra en `$HOME/.mysql_history`. **EVIDENCIAS:**	
4. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Alta**
5. MySQL: **DESCRIPCIÓN:**	**Alta**

TAREA	CRITICIDAD
NOTA: **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	
6. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Alta**
7. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Media**

TAREA	CRITICIDAD
8. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Media**
9. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Media**
10. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:**	**Media**

TAREA	CRITICIDAD
SOLUCIÓN: **EVIDENCIAS:**	

3. VULNERABILIDADES A NIVEL DE ARCHIVOS DE CONFIGURACIÓN CORE

TAREA	CRITICIDAD
1. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Alta**
2. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:**	**Alta**

TAREA	CRITICIDAD
EVIDENCIAS:	
3. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Alta**
4. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Alta**

4. VULNERABILIDADES A NIVEL DE TABLESPACES

TAREA	CRITICIDAD
1. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Alta**
2. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Media**

5. VULNERABILIDADES A NIVEL DE ROLES, USUARIOS Y PRIVILEGIOS

TAREA	CRITICIDAD
1. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Alto**
2. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Medio**
3. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:**	**Media**

TAREA	CRITICIDAD
SOLUCIÓN: **EVIDENCIAS:**	
4. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Alta**

6. VULNERABILIDADES A NIVEL DE CONSIDERACIONES ESPECIALES

TAREA	CRITICIDAD
1. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:**	**Alta**

TAREA	CRITICIDAD
EVIDENCIAS:	
2. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Alta**
3. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Media**
4. MySQL: **DESCRIPCIÓN:** **NOTA:**	**Media**

TAREA	CRITICIDAD
AUDITORIA: **SOLUCIÓN:** **EVIDENCIAS:**	
5. MySQL: **DESCRIPCIÓN:** **NOTA:** **AUDITORIA:** **SOLUCIÓN:** **EVIDENCIAS:**	**Baja**