Documentación Desafió 17

Nombre: Matias O. Riedel

**Objetivo:** Desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI) para una organización que aloja aplicaciones en la nube. Desplegar controles de seguridad que incluyan medidas técnicas, organizativas y de gestión para reducir los riesgos asociados con el alojamiento de aplicaciones en la nube, e incorporar un plan de continuidad del negocio.

**Implementación del Ciclo PDCA**

**1. Plan (Planificar)**

La etapa de planificación implica la creación de un plan estandarizado para aplicar en futuros despliegues, identificando problemas y oportunidades de mejora.

**Aspectos de Seguridad Seleccionados:**

* **Identificación y Autentificación (Objetivo 1):** Asegurar que solo usuarios autorizados puedan acceder al servidor.
  + **Objetivo:** Implementar autenticación multifactor (MFA) para fortalecer la seguridad de acceso.
* **Autorización (Objetivo 2):** Asegurar que los usuarios autenticados solo tengan acceso a los recursos necesarios.
  + **Objetivo:** Configurar roles y permisos usando un principio de privilegio mínimo.

**2. Do (Hacer)**

Implementación y documentación detallada de las tareas planificadas.

1. **Identificación y Autentificación:**

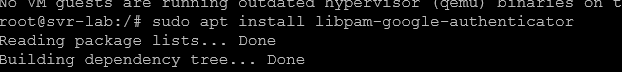
Para el primero paso procederemos a instalar y Configurar el Google Authenticator para MFA, que lo realizaremos de la siguiente manera:

Como primer paso procederemos a actualizar nuestra lista de paquetes con un ‘sudo apt update’

Texto

Descripción generada automáticamente

Una vez actualizada nuestra lista de paquetes procedemos a instalar nuestro aplicativo con el comando ‘sudo apt install libpam-google-authenticator’



Luego de eso, para configurar Google auth para cada usuario en particular cada usuario deberá ejecutar el comando ‘google-authenticator’ para poder realizar la configuración del método de autenticación

Texto

Descripción generada automáticamente

Donde nos aparecerá para proceder con ‘y’ y nos aparecerá lo siguiente para validad con nuestra aplicación de Google auth:

Código QR

Descripción generada automáticamente

Por otro lado procedemos a modificar el PAM para requerir el Google Auth, para esto procedemos a editar el siguienter archivo ‘/etc/pam.d/sshd’



Donde agregaremos la siguiente línea ‘auth required pam\_google\_authenticator.so

’ antes de la línea de ‘@include common-auth’ de la siguiente manera:

Texto

Descripción generada automáticamente

Guardamos el archivo y cerramos el editor

Ahora procederemos a modificar el ‘/etc/ssh/sshd\_config’ para habilitar los desafíos de autenticación

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Donde agregaremos la siguiente línea de código ‘ChallengeResponseAuthentication yes’

Texto

Descripción generada automáticamente

Luego de guardar los cambios procedemos a reiniciar nuestro servicio de sshd con el comando ‘sudo systemctl restart sshd’

1. **Autorización:**

Ahora para esta etapa procederemos a configurar roles y permisos usando ‘sudo’, donde editaremos el archivo sudoers para definir roles y permisos.

Esto lo realizaremos utilizando el comando ‘sudo visudo’ en nuestra consola



Donde se nos abrirá el siguiente archivo para editar

Texto

Descripción generada automáticamente

Dentro del archivo en cuestión llamado ‘sudoers’ agregaremos 2 roles al mismo que serán los siguientes:

# Rol Administrador

%admin ALL=(ALL) ALL

# Rol Auditoría

%auditores ALL=/usr/bin/tail /var/log/auth.log

Los mismos nos quedaran de la siguiente manera

Texto

Descripción generada automáticamente

Luego de tener creados nuestros roles, procedemos a generar los usuarios que tendrán permisos en cada rol especifico utilizando los comandos:

sudo usermod -aG admin mriedel

sudo usermod -aG auditores mati.auditor

Donde los mismos tendrán acceso solo a lo otorgado en sus roles

**Identificación y Autenticación:**

* Evaluar si todos los usuarios han podido configurar correctamente Google Authenticator.
* Verificar logs de autenticación para asegurar que MFA esté funcionando.

**Autorización:**

* Verificar mediante /var/log/auth.log que solo los usuarios apropiados puedan acceder a los recursos.
* Comprobar la eficiencia de los permisos configurados.

**Puntos a Mejorar:**

1. **Documentación de Procesos:** Se recomienda mejorar la documentación sobre la configuración inicial para nuevos empleados.
2. **Automatización:** Evaluar la posibilidad de automatizar la configuración de roles y MFA para reducir errores manuales.

**Checklist para futuros despliegues:**

1. Asegurar la actualización de paquetes:
   * ‘sudo apt update && sudo apt upgrade’
2. Implementar Google Authenticator para MFA:
   * ‘sudo apt install libpam-google-authenticator’
   * ‘google-authenticator’
   * Configuración en ‘/etc/pam.d/sshd’.
   * Configuración en ‘/etc/ssh/sshd\_config’.
   * ‘sudo systemctl restart sshd’
3. Configuración de roles y permisos:
   * Utilizar visudo para editar ‘/etc/sudoers’.
   * Definir roles y permisos.
   * Asignar usuarios a los grupos correspondientes.