Desafío - Seguridad y gestión de SSH en servidores Linux

En este desafío validaremos nuestros conocimientos sobre la configuración segura de SSH y OpenSSH Server, la gestión de claves SSH, las políticas de autenticación y acceso, así como el monitoreo y auditoría de conexiones SSH. Para lograrlo, necesitarás aplicar comandos y configuraciones en servidores Linux.

Lee todo el documento antes de comenzar el desarrollo **grupal de máximo 3 integrantes**, para asegurarte de tener el máximo de puntaje y enfocar bien los esfuerzos.

Descripción

En una empresa de desarrollo tecnológico, los servidores Linux juegan un papel clave en la infraestructura, ya que permiten el acceso remoto a ingenieros, administradores de sistemas y equipos de desarrollo. Sin embargo, recientemente, el equipo de seguridad ha detectado múltiples intentos de acceso no autorizado mediante fuerza bruta y credenciales comprometidas. Esto ha generado una alerta crítica en la empresa, ya que una brecha en SSH podría dar acceso a información confidencial, afectar la disponibilidad de los servicios y comprometer la integridad de la empresa.

Como parte del equipo de seguridad informática, se te ha asignado junto a tu equipo de trabajo la tarea de fortalecer la seguridad de SSH en un servidor crítico de producción. Para ello, deberás aplicar configuraciones seguras en el servicio OpenSSH, implementar autenticación mediante claves SSH, definir políticas estrictas de acceso y habilitar herramientas de monitoreo y auditoría que permitan registrar y analizar los eventos SSH en tiempo real.

Requerimientos

1. **Configuración segura de OpenSSH Server**
   - Modificar el archivo de configuración /etc/ssh/sshd_config para implementar:
     - Cambio del puerto por defecto de SSH.
     - Deshabilitación del acceso root directo.
     - Restricción del acceso solo a usuarios específicos.
     - Configuración de autenticación mediante claves SSH.

   (4 puntos)

2. **Implementación de autenticación con claves SSH**
   - Generar un par de claves SSH y configurar la autenticación sin contraseña.
   - Agregar la clave pública al archivo ~/.ssh/authorized_keys del usuario autorizado.

   (3 puntos)

3. **Monitoreo y auditoría de accesos SSH**
   - Configurar el registro de accesos SSH en /var/log/auth.log o /var/log/secure.
   - Implementar un script que analice los intentos fallidos de autenticación y los almacene en un archivo de auditoría.

   (3 puntos)

 ¡Mucho éxito!

Consideraciones y recomendaciones

- Entrega: Informe en formato PDF con capturas de pantalla, para el requerimiento 1 agregar el archivo de configuración.